GUIDE D'INSTALLATION

FortiGate série 5000
Version 3.0

FORTINET

www.fortinet.com

Guide d'installation FortiGate série 5000
Version 3.0
12 décembre 2005
01-30000-0259-20051212

© Droit d'auteur 2005 Fortinet, Inc. Tous droits réservés. En aucun cas, tout ou partie de cette publication, y compris les textes, exemples, diagrammes ou illustrations, ne peuvent être reproduits, transmis ou traduits, sous aucune forme et d'aucune façon, que ce soit électronique, mécanique, manuelle, optique ou autre, quelqu'en soit l'objectif, sans autorisation préalable de Fortinet, Inc.

Marques déposées
Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyser, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, et FortiWiFi sont des marques déposées de Fortinet, Inc. aux États-Unis et/ou dans d'autres pays. Les noms des sociétés et produits mentionnés ici peuvent être des marques déposées par leurs propriétaires respectifs.

Conformité aux normes
FCC Class A Part 15 CSA/CUS

Attention: Utiliser une batterie du mauvais type pourrait provoquer une explosion. Débarrassez-vous de vos batteries usagées selon la législation locale en vigueur.

Table des Matières

Introduction 6

A propos des distributions internationale et américaine de FortiOS 6

Gamme de Produits Fortinet 7

Services de souscription FortiGuard 7
FortiClient 7
FortiMail 7
FortiAnalyser 8
FortiReporter 8
FortiBridge 8
FortiManager 8

Modules et châssis FortiGate série 5000 9

Châssis FortiGate-5020 9
Châssis FortiGate-5050 9
Châssis FortiGate-5140 9
Module FortiGate-5001 9
Module FortiGate-5001FA2 10
Module FortiGate-5002FB2 10
Carte de Commutation FortiGate-5003 (Switch Blade module) 11
Contrôleur FortiGate de Gestionnaire de Châssis (FortiGate Shelf Management Controller) 11
Alimentation AC du châssis (AC Power shelf) 11

A propos de ce document 12

Conventions utilisées dans ce document 12

Documentation FortiGate 13

Base de Connaissance Fortinet (Fortinet Knowledge Center) 14
Remarques sur la documentation technique Fortinet 14

Service clientèle et support technique 14

Installation des modules FortiGate 15

Avertissements et précautions 16

Les produits de la gamme FortiGate série 5000 17

Châssis FortiGate-5020 17
Châssis FortiGate-5050 19
Châssis FortiGate-5140 21
Module FortiGate-5001 22
Module FortiGate-5001FA2 24
Module FortiGate-5002FB2 25
Carte de Commutation FortiGate-5003 27
Contrôleur de Gestionnaire de Châssis 28

Montage d’un châssis FortiGate série 5000 31

Circulation de l’air 31

Installation d’un module FortiGate-500x 31

Installation des RAM DIMM 31
Installation des transmetteurs SFP 32
Paramétrage des cavaliers 32

Installation d’un module FortiGate-500x 33
Installation d’un module FortiGate-5003 34
Installation du module Gestionnaire de Châssis FortiGate 35
Mise en marche du Gestionnaire de Châssis 35
Ajustement des variables d’environnement 36
Connexion au Contrôleur de Gestionnaire de Châssis 37
Alimentation du châssis 40
Châssis FortiGate-5020 40
Châssis FortiGate-5050 40
Châssis FortiGate-5140 41
Distribution de courant via le FortiGate-5140 42
Module d’alimentation AC du châssis 42
Connexion du FortiGate 44
Interface d’administration web 44
Interface de ligne de commande (CLI) 44
Accès à l’interface d’administration web 44
Connexion à partir de l’interface de ligne de commande 47
Remplacement des modules 48
Echangeabilité à chaud de modules FortiGate-500x 48
Modules d’alimentation de courant échangeables à chaud 49
Paramétrage par défaut 50
Configuration réseau en mode NAT/Route 50
Configuration réseau en mode Transparent 52
Configuration par défaut du pare-feu 52
Profils de protection par défaut 53
Restauration du paramétrage par défaut 54
Restauration du paramétrage par défaut à partir de l’interface d’administration web 54
Restauration du paramétrage par défaut à partir de l’interface de ligne de commande 54
Configuration du FortiGate pour sa mise en réseau 55
Planification de la configuration du FortiGate 55
Mode NAT/Route 55
Mode NAT/Route avec de multiples connexions externes 56
Mode Transparent 57
Installation en mode NAT/Route 58
Préparation de la configuration du FortiGate en mode NAT/Route 58
Configuration DHCP ou PPPoE 59
A partir de l’interface d’administration web 60
A partir de l’interface de ligne de commande 62
Connexion du FortiGate au(x) réseau(x) 64
Configuration des réseaux 65
Installation en mode Transparent 65
Préparation de la configuration du FortiGate en mode Transparent 65
A partir de l’interface d’administration web 66
A partir de l’interface de ligne de commande 67
Connexion du module FortiGate à votre réseau 68

Étapes suivantes **69**

Paramétrage des date et heure 69
Enregistrement de votre FortiGate 70
Mise à jour des signatures antivirus et IPS 70

Logiciel FortiGate 74

Mise à jour logicielle **74**

Mise à jour logicielle à partir de l'interface d'administration web 74
Mise à jour logicielle à partir de l'interface de ligne de commande 75

Retour à une version logicielle antérieure **76**

Retour à une version logicielle antérieure à partir de l'interface d'administration web 76
Retour à une version logicielle antérieure à partir de l'interface de ligne de commande 77

Mise à jour logicielle à partir d'un redémarrage système et par ligne de commande **80**

Restauration de la configuration précédente 82

Test d'une nouvelle version logicielle avant son installation **83**

Index 86

Introduction

Bienvenue et merci d'avoir choisi les produits Fortinet pour la protection en temps réel de votre réseau.

Les boîtiers FortiGate™ Unified Threat Management System (Système de Gestion Unifiée des Attaques) sécurisent les réseaux, réduisent les mauvais usages et abus réseaux et contribuent à une utilisation plus efficace des ressources de communication, sans compromettre la performance de votre réseau. La gamme a reçu les certifications ICSA pare-feu, VPN IPSec et antivirus.

L'appliance FortiGate est un boîtier entièrement dédié à la sécurité. Il est convivial et fournit une gamme complète de services, que ce soit:

- au niveau des applications (comme le filtrage antivirus et le filtrage de contenu).
- au niveau du réseau (comme le pare-feu, la détection et prévention d'intrusion, les VPN et la qualité de service).

Le système FortiGate utilise la technologie de Dynamic Threat Prevention System (Système Dynamique de Prévention des Attaques) (DTPS™). Celle-ci s'appuie sur les dernières avancées technologiques en matière de conception de microcircuits, de gestion de réseaux, de sécurité et d'analyse de contenu. Cette architecture unique basée sur un Asic permet d'analyser en temps réel les contenus applicatifs et les comportements du réseau.

A propos des distributions internationale et américaine de FortiOS

Fortinet produit deux distributions de FortiOS v3.0:

- La distribution internationale est disponible aux utilisateurs en dehors des États-Unis.
- La distribution américaine est disponible à tous les utilisateurs, y compris les utilisateurs aux États-Unis.

La différence principale entre les distributions américaine et internationale réside dans le moteur Antivirus. Le moteur Antivirus valable aux États-Unis analyse le trafic SMTP en mode continu (appelé aussi « mode splice ») et selon un procédé orienté objet. Il utilise également une liste additionnelle de virus privilégiés pour analyser tous les protocoles (HTTP, FTP, IMAP, POP3, SMTP et IM).

Le microcode déployé sur le territoire américain possède les différences suivantes:

- Dans les menus de l'interface d'administration web, **Système > Statut > Statut,** mention est faite de la localisation : « US Domestic » (américain).
- L'analyse des virus du trafic SMTP ne s'opère qu'en mode continu (« mode splice »).
- La fonction de marquage des en-têtes ou sujets des mails identifiés comme SPAM n'est pas disponible.
- Un système de noms de fichiers en quarantaine est généré.
- Le message de remplacement par défaut des mails infectés (« mode splice ») est différent.

Pour davantage d'informations sur les distributions américaine et internationale, reportez-vous au *Guide d'Administration FortiGate*.

Gamme de Produits Fortinet

En complément de sa gamme FortiGate, Fortinet propose une solution complète de logiciels et d'appliances de sécurité, adressant notamment la sécurité de la messagerie, la journalisation et l'édition de rapports statistiques, la gestion du réseau et des configurations. Pour plus d'informations sur les gammes de produits Fortinet, vous pouvez consulter le site www.fortinet.com/products.

Services de souscription FortiGuard

Les services FortiGuard sont des services de sécurité développés, mis à jour et gérés par une équipe de professionnels en sécurité Fortinet. Ces services assurent la détection et le filtrage des attaques, même les plus récentes, pour préserver les ordinateurs et les ressources du réseau. Ces services ont été mis au point à partir des plus récentes technologies de sécurité et sont conçus pour opérer à des coûts opérationnels les plus bas possible.

Les services FortiGuard comprennent:

- Le service FortiGuard antivirus
- Le service FortiGuard IPS (Intrusion Prevention System)
- Le service FortiGuard de filtrage web
- Le service FortiGuard antispam
- Le service FortiGuard premier

Sur notre site web, vous trouverez également un scanner de virus et une encyclopédie des virus et attaques.

FortiClient

Le logiciel FortiClient™ offre un environnement informatique sécurisé et fiable aux utilisateurs d'ordinateurs de bureau et d'ordinateurs portables munis des systèmes d'exploitation les plus répandus de Microsoft Windows. FortiClient offre de nombreuses fonctionnalités, y compris:

- un accès VPN pour se connecter aux réseaux distants
- un antivirus temps réel
- une protection contre des modifications du registre Windows
- une recherche des virus sur tout ou partie du disque dur

FortiClient peut s'installer de façon silencieuse et se déployer aisément sur un parc d'ordinateurs selon un paramétrage pré-établi.

FortiMail

FortiMail™ Secure Messaging Platform (Plate-forme de Sécurisation de Messagerie) fournit une analyse heuristique puissante et flexible, de même que des rapports statistiques sur le trafic de mails entrants et sortants. Le FortiMail met en oeuvre des techniques fiables et hautement performantes pour détecter et

bloquer les mails non désirés, tels que les signatures SHASH (Spam Hash) ou les filtres bayesians. Construit sur base des technologies primées FortiOS et FortiASIC, FortiMail utilise ses pleines capacités d'inspection de contenu afin de détecter les menaces les plus avancées dans les courriers électroniques.

FortiAnalyser

FortiAnalyser™ fournit aux administrateurs réseaux les informations nécessaires qui leur permettent d'assurer une meilleure protection du réseau, une plus grande sécurité contre attaques et vulnérabilités. FortiAnalyser permet entre autres:

- de centraliser les journaux des boîtiers FortiGate et des serveurs syslog
- de générer des centaines de rapports à partir des données collectées
- de scanner le réseau et générer des rapports de vulnérabilités
- de stocker les fichiers mis en quarantaine par FortiGate

FortiAnalyser peut également être configuré en sniffer réseau et capturer en temps réel le trafic intercepté. Vous pouvez en outre utiliser FortiAnalyser comme lieu de stockage où les utilisateurs peuvent accéder et partager des données, telles que des rapports et journaux conservés sur son disque dur.

FortiReporter

Le logiciel FortiReporter™ Security Analyzer génère des rapports explicites. Il peut centraliser des journaux de n'importe quel boîtier FortiGate, ainsi que de plus de 30 boîtiers de réseau et de sécurité provenant de constructeurs tiers. FortiReporter offre une visibilité sur les abus réseau, l'utilisation de la bande passante et l'usage du web afin de s'assurer que le réseau est utilisé de façon appropriée. FortiReporter permet aux administrateurs d'identifier les attaques et d'y répondre. Il permet également de définir des actions proactives de protection des réseaux avant que ceux-ci ne soient confrontés à une augmentation des menaces.

FortiBridge

FortiBridge™ permet d'assurer une continuité de connexion réseau même en cas de panne électrique d'un système FortiGate. Le FortiBridge connecté en parallèle au FortiGate dévie le flux réseau lorsqu'il détecte une panne sur le boîtier et reçoit alors le trafic pour éviter toute coupure réseau. FortiBridge est facile à utiliser et à déployer. Vous pouvez programmer à l'avance les actions que FortiBridge mettra en place en cas de panne de courant ou de panne dans le système FortiGate.

FortiManager

FortiManager™ est conçu pour répondre aux besoins des grandes entreprises (y compris les fournisseurs de services de gestion de sécurité) responsables du déploiement et du maintien de dispositifs de sécurité à travers un parc d'équipements FortiGate. FortiManager vous permet de configurer et de contrôler les statuts de plusieurs boîtiers FortiGate. Vous pouvez également consulter leurs journaux en temps réel et leurs historiques, ou encore émettre les versions du microcode FortiOS. FortiManager est facile à utiliser et s'intègre aisément à des systèmes tiers.

Modules et châssis FortiGate série 5000

Les plates-formes de sécurité réseau FortiGate série 5000 sont des systèmes basés sur des châssis destinés aux grandes entreprises et fournisseurs de services haut débit Internet. Ils garantissent des services de sécurité intégrant pare-feu, VPN, protection antivirus, antispam, filtrage du contenu web et système de prévention d'intrusion (IPS). Le grand choix de configurations système qu'offrent les FortiGate série 5000 assure la flexibilité nécessaire à la croissance des réseaux de haute performance. Les châssis FortiGate série 5000 supportent de multiples modules FortiGate série 5000 ainsi que des sources d'alimentation échangeables à chaud.

Cette approche modulaire offre aux entreprises et utilisateurs des FAI (Fournisseurs d'accès Internet) une solution adaptable hautement performante et tolérante aux pannes. La gamme de produits FortiGate série 5000 présente trois modèles de châssis.

Châssis FortiGate-5020

Le châssis FortiGate-5020 comprend deux slots (logements) permettant l'installation de deux modules pare-feu antivirus FortiGate-5000. Pour plus de détails, reportez-vous à « Châssis FortiGate-5020 » à la page 17.

Châssis FortiGate-5050

Le châssis FortiGate-5050 comprend cinq slots permettant d'installer jusqu'à cinq modules pare-feu antivirus FortiGate-5000. Il est également possible d'installer deux Cartes de Commutation FortiGate-5003 et trois modules FortiGate-5000 ou toute autre combinaison désirée. Ce châssis peut connecter jusqu'à deux Gestionnaires de Châssis et un module optionnel de conversion d'alimentation. Pour plus de détails, reportez-vous à « Châssis FortiGate-5050 » à la page 19.

Châssis FortiGate-5140

Le châssis FortiGate-5140 comprend quatorze slots permettant d'installer jusqu'à quatorze modules pare-feu antivirus FortiGate-5000. Il est également possible d'installer une voire deux Cartes de Commutation FortiGate-5003, ou encore toutes combinaisons faites de maximum douze modules pare-feu antivirus FortiGate-500x et deux cartes FortiGate-5003. Ce châssis peut connecter jusqu'à deux Gestionnaires de Châssis et un module optionnel de conversion d'alimentation. Pour plus de détails, reportez-vous à « Châssis FortiGate-5140 » à la page 21.

Module FortiGate-5001

Chaque module FortiGate-5001 est un système autonome de sécurité réseau hautement performant qui supporte des fonctionnalités exigeantes telles que des VLAN 802.1Q et domaines virtuels multiples, opérant à la vitesse du réseau.
Le module FortiGate-5001 comprend :

- Quatre interfaces réseau gigabits en fibre optique
- Quatre interfaces réseau cuivre 10/100/1000
- Une connexion console série DB-9

- Deux connexions USB
- Deux RAM DIMM
- Deux leviers d'extraction pour aligner le FortiGate-5001 dans le châssis FortiGate
- Deux attaches de montage pour fixer le module au châssis de manière sécurisée

Plusieurs modules FortiGate-5001 peuvent être regroupés dans un cluster haute disponibilité (HA) assurant ainsi un partage de charge entre les unités et une redondance matérielle.
Le clustering haute disponibilité requiert deux interfaces gigabits internes pour la communication haute disponibilité, ce qui laisse les huit interfaces gigabits du panneau avant disponibles pour les connexions réseau. Pour plus de détails sur le FortiGate-5001, reportez-vous à « Module FortiGate-5001 », à la page 22.

Module FortiGate-5001FA2

Chaque module FortiGate-5001FA2 est un système autonome de sécurité réseau hautement performant qui supporte des fonctionnalités exigeantes telles que des VLAN 802.1Q et domaines virtuels multiples, opérant à la vitesse du réseau.

Le module FortiGate-5001FA2 comprend :

- Quatre interfaces réseau gigabits en fibre optique
  - Ports 3 et 4 incluant un traitement haute performance des petits paquets
- Quatre interfaces cuivre 10/100/1000
- Une connexion console série DB-9
- Deux connexions USB
- Deux RAM DIMM
- Deux leviers d'extraction pour aligner le FortiGate-5001FA2 dans le châssis FortiGate
- Deux attaches de montage pour fixer le module au châssis de manière sécurisée

Plusieurs modules FortiGate-5001FA2 peuvent être regroupés dans un cluster haute disponibilité (HA) assurant ainsi un partage de charge entre les unités et une redondance matérielle.
Le clustering haute disponibilité requiert deux interfaces gigabits internes pour la communication haute disponibilité, ce qui laisse les huit interfaces gigabits du panneau avant disponibles pour les connexions réseau. Pour plus de détails sur le FortiGate-5001FA2, reportez-vous à « Module FortiGate-5001FA2 », à la page 24.

Module FortiGate-5002FB2

Chaque module FortiGate-5002FB2 est un système autonome de sécurité réseau hautement performant qui supporte des fonctionnalités exigeantes telles que des VLAN 802.1Q et domaines virtuels multiples, opérant à la vitesse du réseau.

Le module FortiGate-5002FB2 comprend :

- Six interfaces réseau cuivre 10/100/1000, y compris deux ports SFP
- Une connexion console série DB-9
- Deux connexions USB
- Deux RAM DIMM

- Deux leviers d'extraction pour aligner le FortiGate-5002FB2 dans le châssis FortiGate
- Deux attaches de montage pour fixer le module au châssis de manière sécurisée

Plusieurs modules FortiGate-5002FB2 peuvent être regroupés dans un cluster haute disponibilité (HA) assurant ainsi un partage de charge entre les unités et une redondance matérielle.
Le clustering haute disponibilité requiert deux interfaces gigabit internes pour la communication haute disponibilité, ce qui laisse les six interfaces gigabit du panneau avant disponibles pour les connexions réseau. Pour plus de détails sur le FortiGate-5002FB2, reportez-vous à « Module FortiGate-5002FB2 », à la page 25.

Carte de Commutation FortiGate-5003 (Switch Blade module)

La carte de commutation FortiGate-5003 est un composant haute disponibilité qui, lorsqu'il est connecté aux châssis FortiGate-5050 ou FortiGate-5140, fournit toutes les performances d'un clustering haute disponibilité, que ce soit entre modules FortiGate-5001 ou entre châssis FortiGate-5050 et FortiGate-5140.

Le module FortiGate-5003 comprend :

- Seize ports gigabits Ethernet, dont :
  - Treize interfaces gigabits internes de fond de panier
  - Trois interfaces externes 10/100/1000 pour la connexion à d'autres châssis
- Un port 10/100 de gestion hors bande
- Un accès console RJ-45
- Des indicateurs LED
- Deux leviers d'extraction pour aligner le FortiGate-5003 dans le châssis FortiGate.

Pour plus de détails, reportez-vous à « Carte de Commutation FortiGate-5003 » à la page 27.

Contrôleur FortiGate de Gestionnaire de Châssis (FortiGate Shelf Management Controller)

Le module Contrôleur FortiGate de Gestionnaire de Châssis est responsable de l'alimentation d'un châssis et du traitement des ajouts et retraits de modules, y compris l'échange de ressources interconnectées, la gestion de la distribution du courant, du refroidissement et des statuts du châssis. Pour plus de détails, reportez-vous à « Connexion au Contrôleur FortiGate de Gestionnaire de Châssis » à la page 37.

Alimentation AC du châssis (AC Power shelf)

Ce module fournit le moyen de convertir le courant alternatif (AC) en courant continu (DC) pour les châssis FortiGate-5050 et FortiGate-5140. Il inclut de multiples modules de courant assurant ainsi une redondance et une échangeabilité à chaud des sources de courant. Pour plus de détails, reportez-vous à « Alimentation AC du châssis » à la page 42.

A propos de ce document

Ce guide d'installation procure les informations nécessaires à l'installation des châssis et modules FortiGate-5000 et à la configuration sur vos réseaux.

Ce document comprend les chapitres suivants :

- Installation des modules FortiGate – Décrit le déballage, l'installation et le démarrage des modules et châssis FortiGate.
- Configuration du FortiGate pour sa mise en réseau – Fournit un aperçu des modes de fonctionnement des cartes pare-feu antivirus FortiGate et explique comment intégrer le FortiGate au réseau.
- Logiciel FortiGate – Décrit comment installer, mettre à jour, restaurer et tester le microcode de l'équipement FortiGate.
- Paramétrage par défaut – Fournit les paramètres par défaut de tous les modules FortiGate série 5000.

Conventions utilisées dans ce document

Les conventions suivantes sont utilisées dans ce guide :

- Dans les exemples, les adresses IP privées sont utilisées aussi bien pour les adresses IP privées que publiques.
- Les remarques et attentions fournissent des informations importantes :

Les « **remarques »** vous apportent de l'information additionnelle utile.

Les « **attentions »** vous mettent en garde contre des commandes et procédures qui pourraient avoir des résultats inattendus ou indésirables tels que perte de données ou détérioration de l'équipement.

Conventions typographiques

La documentation du FortiGate utilise les conventions typographiques suivantes :

Convention	Exemple
Entrée clavier	**Dans le champ** Nom de Passerelle**, tapez un nom pour le client VPN distant (par exemple, `Central_Office_1`).**

Exemple de code	`config sys global`
	`set ips-open enable`
	`end`

Syntaxe CLI (Interface de ligne de commande)	`config firewall policy`
	`edit id_integer`
	`set http_retry_count <retry_integer>`
	`set natip <address_ipv4mask>`
	`end`

Nom des documents	***Guide d'Administration FortiGate***
Commande de Menus	**Allez** sur VPN > IPSEC **et sélectionnez Créer Phase 1.**
Affichage du résultat d'un programme	`Welcome!`
Variable	`<address_ipv4>`

Documentation FortiGate

Les versions les plus récentes de la documentation Fortinet, de même que les précédentes parutions, sont disponibles sur le site de documentation technique Fortinet à l'adresse http://docs.forticare.com.

Les guides suivants y sont disponibles en anglais. Certains guides sont ou seront aussi disponibles en français :

- *FortiGate QuickStartGuide - Guide de démarrage rapide FortiGate*
  Fournit les informations de base sur la connexion et l'installation d'un FortiGate
- *FortiGate Install Guide - Guide d'Installation FortiGate*
  Décrit comment installer un FortiGate. Il comprend des informations sur le matériel, des informations sur la configuration par défaut, ainsi que des procédures d'installation, de connexion et de configuration de base. Sélectionnez le guide en fonction du numéro du modèle du produit.
- *FortiGate Administration Guide - Guide d'Administration FortiGate*
  Fournit les informations de base sur la manière de configurer un FortiGate, y compris la définition des profils de protection FortiGate et des règles pare-feu. Explique comment appliquer les services de prévention d'intrusion, protection antivirus, filtrage web et filtrage antispam (antipollupostage). Parcourt également la manière de configurer un VPN.
- *FortiGate online help - Aide en ligne FortiGate*
  Fournit le *Guide d'Administration* au format HTML avec des outils de recherche. Vous pouvez accéder à l'aide en ligne à partir de l'interface d'administration web.
- *FortiGate CLI Reference - Guide de Référence CLI*
  Décrit comment utiliser l'interface de ligne de commande FortiGate et répertorie toutes ses commandes.
- *FortiGate Log Message Reference - Guide de référence des messages journalisés d'un FortiGate*
  Disponible uniquement à partir de la base de connaissance (Fortinet Knowledge Center), ce mode d'emploi décrit la structure et le contenu des messages présents dans les journaux FortiGate.
- *FortiGate High Availability User Guide - Guide utilisateur des fonctions de haute disponibilité FortiGate*
  Fournit une description détaillée des fonctions de haute disponibilité et du protocole de clustering FortiGate.
- *FortiGate IPS User Guide - Guide utilisateur de l'IPS FortiGate (Système de Prévention d'Intrusion)*
  Décrit la configuration des paramètres IPS FortiGate et le traitement des attaques les plus courantes.
- *FortiGate IPSec VPN User Guide - Guide utilisateur des VPN IPSec FortiGate*
  Fournit des instructions pas à pas sur la configuration VPN IPSec via l'interface d'administration web.
- *FortiGate SSL VPN User Guide - Guide utilisateur du VPN SSL FortiGate*
  Compare les technologies FortiGate VPN IPSec et VPN SSL et décrit comment configurer à partir de l'interface graphique les modes VPN SSL web et VPN SSL tunnel pour les connexions à distance des utilisateurs.
- *FortiGate PPTP VPN User Guide - Guide utilisateur du VPN PPTP FortiGate*
  Explique comment configurer un VPN PPTP via l'interface d'administration web.
- *FortiGate Certificate Management User Guide - Guide utilisateur de gestion des certificats FortiGate*
  Indique comment gérer les certificats digitaux, et notamment comment générer des requêtes de certificat, installer des certificats, importer le certificat de

l'autorité de certification et des listes de révocation, sauvegarder et restaurer des certificats et leurs clefs privées associées.

- *FortiGate VLANs and VDOMs User Guide - Guide utilisateur des VLAN et VDOM FortiGate*

  Décrit comment configurer des VLAN et VDOM en mode NAT/Route et Transparent. Des exemples détaillés y sont repris.

Base de Connaissance Fortinet (Fortinet Knowledge Center)

De la documentation technique complémentaire est disponible dans la base de connaissance Fortinet (Fortinet Knowledge Center), notamment des articles sur les dépannages et questions les plus fréquemment rencontrés, des notes techniques, et davantage. Vous pouvez consulter le site de la Base de Connaissance Fortinet à l'adresse http://kc.forticare.com.

Remarques sur la documentation technique Fortinet

Merci d'indiquer toute éventuelle erreur ou omission trouvée dans cette documentation à techdoc@fortinet.com.

Service clientèle et support technique

Le Support Technique Fortinet (Fortinet Technical Support) propose son assistance pour une installation rapide, une configuration facile et une fiabilité des systèmes Fortinet.

Pour connaître ces services, consultez le site de Support Technique Fortinet à l'adresse http://support.fortinet.com.

Installation des modules FortiGate

Cette section couvre l'installation et le déploiement des châssis et modules FortiGate-5000 sur votre réseau. Vous y retrouverez les sujets suivants :

- Avertissements et précautions
- Les produits de la gamme FortiGate série 5000
- Montage d'un châssis FortiGate série 5000
- Installation d'un module FortiGate-500x
- Installation d'un module FortiGate-5003
- Installation du module Gestionnaire de Châssis FortiGate
- Alimentation du châssis
- Connexion du FortiGate
- Remplacement des modules

Avertissements et précautions

Les procédures décrites dans ce chapitre s'adressent à un personnel technique qualifié ayant de l'expérience dans l'installation et la configuration de serveurs. Avant de commencer, il est nécessaire de lire et d'adhérer à tous les avertissements et remarques de ce chapitre.

Attention : Soyez attentifs aux remarques et avertissements avant d'opérer le pare-feu antivirus FortiGate.

- Fermer tous les interrupteurs de courant ne supprime pas forcément totalement la présence de courant dans le boîtier FortiGate. Déconnectez le FortiGate de sa source d'alimentation, de ses connexions et réseaux de télécommunication avant d'installer et retirer les composants FortiGate ou d'exécuter d'autres tâches de maintenance. En cas de non respect de ces mesures de prudence, vous risquez de vous blesser ou d'endommager les équipements. Certains circuits du FortiGate peuvent en effet continuer d'opérer alors que toutes les alimentations sont coupées.
- Installer le châssis FortiGate dans les étages inférieurs de l'armoire rack afin d'éviter d'alourdir le haut de l'armoire et de risquer une chute.
- Ne jamais insérer d'objets ou d'outils métalliques dans les logements, emplacements et slots ouverts.
- Des décharges électrostatiques (DES) peuvent endommager vos modules FortiGate. Les procédures suivantes doivent être appliquées dans une zone antistatique. En cas d'indisponibilité d'une telle zone, protégez-vous des décharges en portant un bracelet antistatique attaché à une surface métallique du châssis FortiGate.
- Le FortiGate pourrait surcharger votre circuit d'alimentation et impacter votre protection de surcourant et le câblage d'alimentation. Utilisez un étiquetage approprié pour solliciter la prudence.
- Assurez-vous que le FortiGate a une prise de terre fiable. Fortinet recommande une connexion directe au secteur.
- Si vous installez un châssis FortiGate dans un assemblage multi racks ou dans une armoire rack fermée, la température ambiante de l'armoire rack risque d'être plus élevée que la température ambiante de la pièce. Assurez-vous toujours que la température ambiante ne dépasse pas la température maximum indiquée par le constructeur.

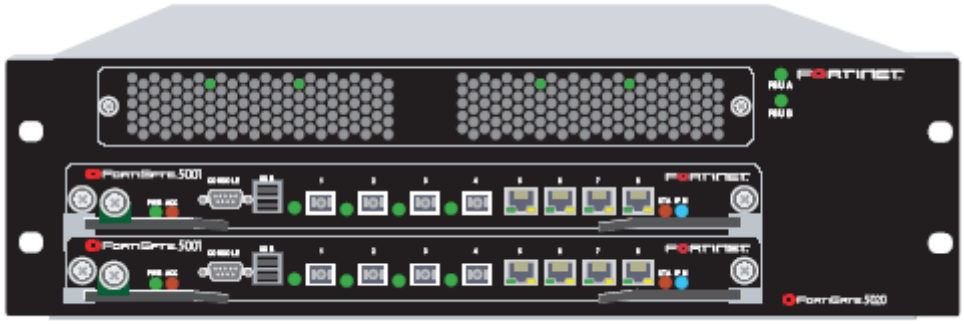
Les produits de la gamme FortiGate série 5000

Les produits de la gamme FortiGate série 5000 comprennent un assortiment de châssis et modules à slots multiples, y compris :

- Châssis FortiGate-5020
- Châssis FortiGate-5050
- Châssis FortiGate-5140
- Module FortiGate-5001
- Module FortiGate-5001FA2
- Module FortiGate-5002FB2
- Carte de Commutation FortiGate-5003
- Contrôleur de Gestionnaire de Châssis
- Module d'alimentation AC du châssis

Châssis FortiGate-5020

Illustration 1 : Le châssis FortiGate-5020 avec deux modules FortiGate-5001



Le châssis FortiGate-5020 peut être monté dans un rack standard de 19 pouces, la hauteur du châssis étant de 4U.

Il possède les fonctionnalités suivantes:

- peut inclure jusqu'à deux modules pare-feu antivirus FortiGate-500x
- supporte l'échangeabilité à chaud des modules pare-feu antivirus FortiGate-500x et des alimentations de courant
- comprend un refroidissement interne
- possède des alimentations de courant redondantes pour une plus grande fiabilité

Tableau 1 : Description des caractéristiques physiques du châssis FortiGate-5020

Dimensions	**13.3 x 43.2 x 39.4 cm (5.25 x 17 x 15.5 pouces) (H x L x P)**
Poids	**16.1 kg (35.5 livres)**
Environnement opérationnel	**Température : -25 à 70°C (-13 à 158°F)**
	Humidité relative : 5 à 95% (non condensée)
Environnement de stockage	**Température : -20 à 80°C**
	Humidité relative : 5 à 95% (non condensée)
Dissipation de la puissance	**Maximum : 800 watts**
Alimentations	**2 ensembles de conversion 100-240 VAC en 48 VDC redondants**

Fonctionnalités du panneau avant

L'illustration 1 reprend la localisation des modules sur le panneau avant du FortiGate-5020. Le panneau avant prévoit l'accès pour un ou deux modules pare-feu antivirus FortiGate-500x. Deux alimentations de courant redondantes sont installées derrière le panneau d'alimentation amovible.

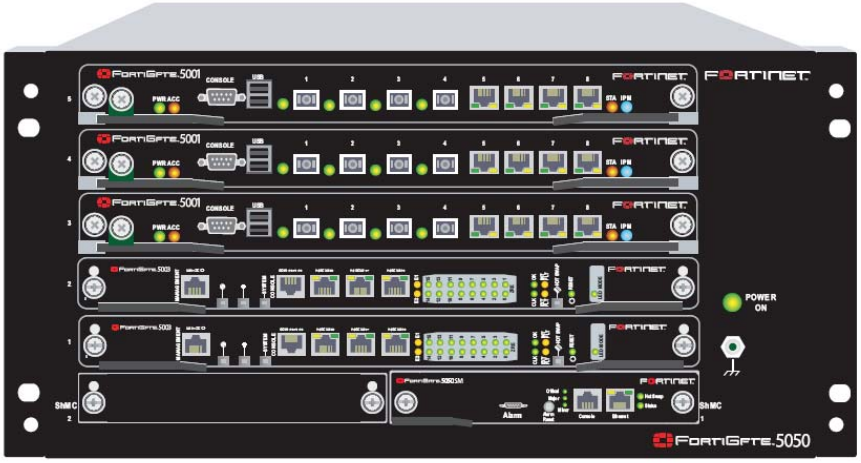
Attention : Ne pas faire fonctionner le châssis FortiGate-5020 avec des slots ouverts sur le panneau avant. Pour un refroidissement et une sécurité optimum, les slots doivent contenir un module pare-feu antivirus FortiGate série 5000 ou, à défaut, un couvercle. De plus, le panneau d'alimentation amovible doit être remis en place.

Tableau 2 : Les indicateurs des diodes électroluminescentes du châssis FortiGate-5020

Diodes	Etat	Description
PSU A	**Vert**	**L'alimentation de courant A est opérationnelle et fonctionne correctement.**
PSU B	**Vert**	**L'alimentation de courant B est opérationnelle et fonctionne correctement.**

Châssis FortiGate-5050

Illustration 2 : Châssis FortiGate-5050 avec des modules FortiGate-5001, FortiGate-5003 et FortiGate-5050SM.



Le châssis FortiGate-5050 peut être monté dans un rack standard de 19 pouces, la hauteur du châssis étant de 5U.

Il possède les fonctionnalités suivantes:

- peut inclure une des combinaisons suivantes :
  - jusqu'à cinq modules pare-feu antivirus FortiGate-500x
  - un FortiGate-5003 et jusqu'à quatre modules FortiGate-500x
  - deux FortiGate-5003 et jusqu'à trois modules FortiGate-500x
- supporte l'échangeabilité à chaud des modules et alimentations de courant
- comprend un refroidissement interne
- possède des alimentations de courant redondantes pour une plus grande fiabilité
- inclut le Contrôleur de Gestionnaire de Châssis FortiGate-5050SM avec un second FortiGate-5050SM optionnel redondant.

Tableau 3 : Description des caractéristiques physiques du châssis FortiGate-5050

Dimensions	**22.2 x 43.2 x 39.4 cm (8.75 x 17 x 15.5 pouces) (H x L x P)**
Poids	**12.1 kg (26.75 livres)**
Environnement opérationnel	**Température : 0 à 40°C (32 à 104°F)**
	Humidité relative : 5 à 95% (non condensée)
Environnement de stockage	**Température : -25 à 70°C (-13 à 158°F)**
	Humidité relative : 5 à 95% (non condensée)
Puissance consommée	**Maximum : 1135 W DC**
Puissance en entrée	**2 x 48V – 58V DC redondants**

Fonctionnalités du panneau avant

L'illustration 2 reprend la localisation des composants sur le panneau avant du FortiGate-5050. Le panneau avant prévoit l'accès de modules pare-feu antivirus FortiGate-500x, FortiGate-5003 et gestionnaires de châssis FortiGate. Deux alimentations de courant redondantes sont installées derrière le panneau d'alimentation amovible.

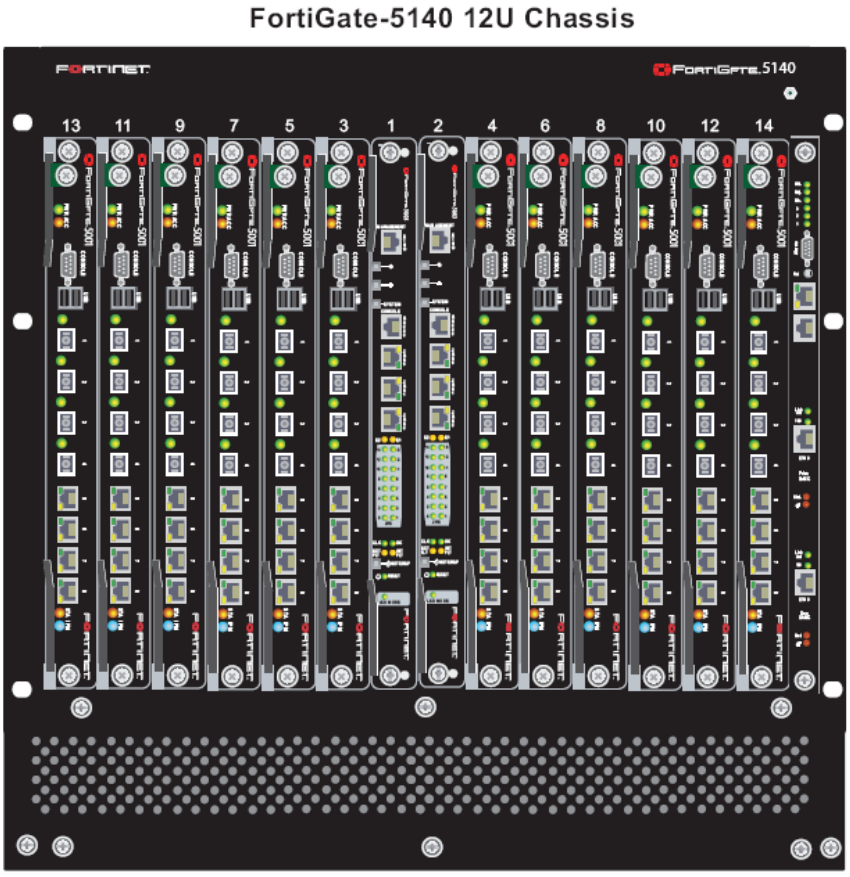
Attention : Ne pas faire fonctionner le châssis FortiGate-5050 avec des slots ouverts sur le panneau avant. Pour un refroidissement et une sécurité optimum, les slots doivent contenir un module FortiGate-500x ou, à défaut, un couvercle. De plus, le panneau d'alimentation amovible doit être remis en place.

Tableau 4 : Les indicateurs des diodes électroluminescentes du châssis FortiGate-5050

Diodes	Etat	Description
Power On	**Vert**	**L'alimentation de courant est opérationnelle et fonctionne correctement.**

Châssis FortiGate-5140

Illustration 3 : Panneau avant du châssis FortiGate-5140



Il possède les fonctionnalités suivantes:

- peut inclure toute combinaison de modules pare-feu antivirus FortiGate-500x et jusqu'à deux modules FortiGate-5003 pour remplir les 14 slots disponibles.
- supporte l'échangeabilité à chaud de modules pare-feu antivirus FortiGate-500x, de plateaux de ventilateurs et d'alimentations de courant
- comprend un refroidissement interne
- possède des alimentations de courant redondantes pour une plus grande fiabilité
- inclut le Contrôleur de Gestionnaire de Châssis FortiGate-5140SM

Tableau 5 : Description des caractéristiques physiques du châssis FortiGate-5140

Dimensions	**53.3 x 48.3 x 42.7 cm (21 x 19 x 16.8 pouces) (H x L x P)**
Poids	**29.3 kg (64.5 livres)**
Environnement opérationnel	**Température : 0 à 40°C (32 à 104°F)**
	Humidité relative : 5 à 95% (non condensée)
Environnement de stockage	**Température : -25 à 70°C (-13 à 158°F)**
	Humidité relative : 5 à 95% (non condensée)
Puissance consommée	**Maximum : 2980 W DC**
Puissance en entrée	**2 x 48V – 58 V DC redondants**

Fonctionnalités du panneau avant

L'illustration 3 reprend la localisation des composants sur le panneau avant du FortiGate-5140. Le panneau avant prévoit l'accès aux modules FortiGate-5001 et FortiGate-5003. Deux alimentations de courant redondantes sont installées derrière le panneau d'alimentation amovible au dos du châssis.

Attention : Ne pas faire fonctionner le châssis FortiGate-5140 avec des slots ouverts sur le panneau avant. Pour un refroidissement et une sécurité optimums, les slots doivent contenir un module FortiGate-500x ou, à défaut, un couvercle. De plus, le panneau d'alimentation amovible doit être remis en place.

Module FortiGate-5001

Tous les châssis FortiGate peuvent inclure au moins un module FortiGate-5001. Celui-ci peut fonctionner comme système autonome de gestion des menaces (Universal Threat Management System) ou faire partie d'un cluster HA FortiGate-5001.

Illustration 4 : Le panneau avant du FortiGate-5001

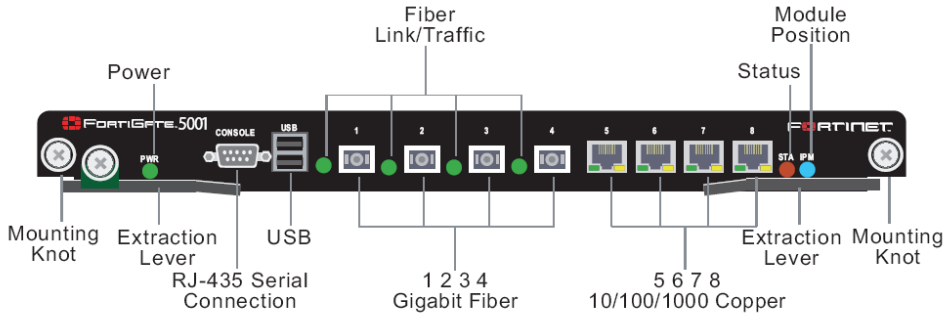


Tableau 6 : Les indicateurs des diodes électroluminescentes du module FortiGate-5001

Diode	État	Description
PWR	**Vert**	**Le module FortiGate-5001 est sous tension.**
STA	**Vert**	**Le module FortiGate-5001 opère normalement.**
	Rouge	**Le FortiGate-5001 s'initialise ou présente une erreur.**
IPM	**Bleu**	**Le FortiGate-5001 est prêt à être échangé à chaud (ou la carte est prête à être retirée du châssis).**
	Bleu – clignotant	**Le FortiGate-5001 passe du mode hot swap (échangeabilité à chaud) au mode de fonctionnement normal ou vice-versa.**
	Éteint	**Opère normalement. Le module FortiGate-5001 est en contact avec le fond de panier du châssis FortiGate.**
1, 2, 3, 4	**Vert**	**La jarretière fibre optique appropriée est connectée à l'interface gigabits fibre.**
	Clignotant	**Activité réseau présente sur l'interface gigabits fibre.**
5, 6, 7, 8	**Vert**	**Le câble approprié est connecté à l'interface cuivre 10/100/1000 et l'équipement connecté est alimenté.**
	Clignotant	**Activité réseau présente sur cette interface.**
	Ambre	**L'interface est connectée à 1000 Mbit/s.**

Connexions

Les connexions interface suivantes sont disponibles sur le module FortiGate-5001.

Connecteur	Type	Vitesse	Protocole	Description
1, 2, 3, 4	**LC SFP**	**1000Base-SX**	**Ethernet**	**Connexions fibre optique multimode vers réseaux optiques gigabit. Le FortiGate-5001 est fourni avec 4 connecteurs SFP à insérer dans les emplacements 1-4 du panneau avant.**
5, 6, 7, 8	**RJ-45**	**1000Base-T**	**Ethernet**	**Connexion gigabit cuivre vers réseaux cuivre 10/100/1000.**
CONSOLE	**DB-9**	**9600 bit/s**	**Série RS-232**	**Connexion série vers l'interface de ligne de commande.**

Module FortiGate-5001FA2

Tous les châssis FortiGate peuvent inclure au moins un module FortiGate-5001FA2. Celui-ci fonctionne comme un système autonome de gestion des menaces (Universal Threat Management System) ou peut faire partie d'un cluster HA FortiGate-5001FA2. Ce module comprend les mêmes protections pare-feu que le FortiGate-5001, à l'exception d'un petit co-processeur de paquet sur les ports 3 et 4 qui procure une accélération des performances.

Illustration 5 : panneau avant du FortiGate-5001FA2

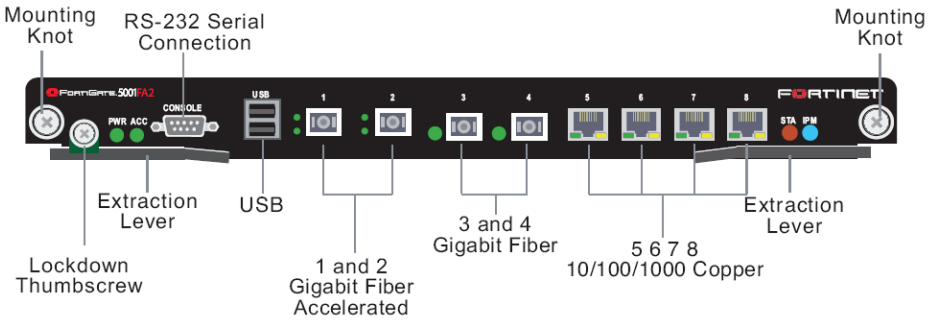


Tableau 7 : Les indicateurs des diodes électroluminescentes du module FortiGate-5001FA2

Diode	État	Description
PWR	**Vert**	**Le module FortiGate-5001FA2 est sous tensio**
STA	**Vert**	**Le module FortiGate-5001FA2 opère normalement.**
	Rouge	**Le FortiGate-5001FA2 s'initialise ou présente une erreur.**
IPM	**Bleu**	**Le FortiGate-5001FA2 est prêt à être débranché à chaud (ou la carte est prête à être retirée du châssis). .**
	Bleu – clignotant	**Le FortiGate-5001FA2 passe du mode hot swap (débranchement à chaud) au mode de fonctionnement normal ou vice-versa.**
	Éteint	**Opère normalement. Le module FortiGate-5001FA2 est en contact avec le fond de panier du châssis FortiGate.**
1, 2, 3, 4	**Vert**	**La jarretière fibre optique appropriée est connectée à l'interface gigabits fibre.**
	Clignotant	**Activité réseau présente sur l'interface gigabits fibre.**
5, 6, 7, 8	**Vert**	**Le câble approprié est connecté à l'interface cuivre 10/100/1000 et l'équipement connecté est alimenté.**
	Clignotant	**Activité réseau présente sur cette interface.**
	Ambre	**L'interface est connectée à 1000 Mbit/s.**

Connexions

Le module FortiGate-5001FA2 présente les connexions interface suivantes.

Connecteur	Type	Vitesse	Protocole	Description
1 et 2	**LC SFP**	**1000Base-SX**	**Ethernet**	**Connexions fibre optique multimode vers réseaux optiques gigabit.**
3 et 4	**LC SFP**	**1000Base-SX**	**Ethernet**	**Améliore la performance de petits paquets sur connexions fibre optique multimode vers réseaux optiques gigabit.**
5, 6, 7, 8	**RJ-45**	**1000Base-T**	**Ethernet**	**Connexion gigabit en cuivre vers réseaux cuivre 10/100/1000.**
CONSOLE	**DB-9**	**9600 bit/s**	**Série RS-232**	**Connexion série vers l'interface de ligne de commande.**

Le FortiGate-5001FA2 est fourni avec 4 connecteurs SFP (Small Formfactor Pluggable) à insérer dans les emplacements 1-4 du panneau avant.

Performance pour les petits paquets

Les ports 3 et 4 du module FortiGate-5001FA2 comprennent un co-processeur SPP (Small Packet Performance) qui augmente significativement la performance pour les paquets inférieurs à 512 octets. De plus ce co-processeur permet au module FortiGate-5001FA2 d'atteindre une performance proche des performances nominales de la ligne pour ces paquets. Les applications utilisant de petits paquets, telles que le protocole http et les mails, profiteront de cette accélération.

Les quatre autres ports servent aux applications utilisant des paquets de plus grandes tailles telles que les transferts FTP, les copies de fichiers et les accès basés serveurs.

Module FortiGate-5002FB2

Tous les châssis FortiGate peuvent inclure au moins un module FortiGate-5002FB2. Celui-ci fonctionne également comme un système autonome de gestion de menaces (Universal Threat Management System) ou peut faire partie d'un cluster HA FortiGate-5002FB2. Ce module comprend la même protection pare-feu que le FortiGate-5001, à l'exception des deux ports SFP.

Illustration 6 : Panneau avant du FortiGate-5002FB2

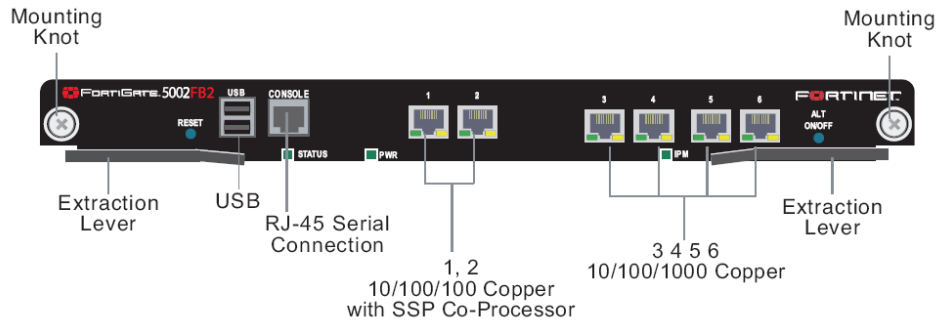


Tableau 8 : Les indicateurs des diodes électroluminescentes du module FortiGate-5002FB2

Diode	État	Description
PWR	**Vert**	**Le module FortiGate-5002FB2 est sous tensior**
STA	**Vert**	**Le module FortiGate-5002FB2 opère normalement.**
	Rouge	**Le FortiGate-5002FB2 s'initialise ou présente une erreur.**
IPM	**Bleu**	**Le FortiGate-5002FB2 est prêt à être débranché à chaud (ou la carte est prête à être retirée du châssis). .**
	Bleu – clignotant	**Le FortiGate-5002FB2 passe du mode hot swap (débranchement à chaud) au mode de fonctionnement normal ou vice-versa.**
	Éteint	**Opère normalement. Le module FortiGate-5002FB2 est en contact avec le fond de panier du châssis FortiGate.**
Ports 1-6	**Vert**	**Le câble approprié est connecté à l'interface cuivre 10/100/1000 et l'équipement connecté est alimenté.**
	Clignotant	**Activité réseau présente sur l'interface gigabits fibre.**
	Ambre	**L'interface est connectée à 1000 Mbit/s.**

Connexions

Les connexions interface suivantes sont disponibles sur le module FortiGate-5002FB2.

Connecteur	Type	Vitesse	Protocole	Description
1 et 2 (ports améliorés)	**RJ-45**	**1000Base-T**	**Ethernet**	**Connexion gigabit en cuivre vers réseaux cuivre 10/100/1000. Les ports sont améliorés avec des co-processeurs SPP.**
3, 4, 5, 6	**RJ-45**	**1000Base-T**	**Ethernet**	**Connexion gigabit en cuivre vers réseaux cuivre 10/100/1000. Les ports ne sont pas améliorés avec les co-processeurs SPP.**
CONSOLE	**RJ-45**	**9600 bit/s**	**Série RS-232**	**Connexion série vers l'interface de ligne de commande.**

Performance pour les petits paquets

Les ports 1 et 2 du module FortiGate-5002FB2 comprennent un co-processeur SPP (Small Packet Performance) qui augmente significativement la performance pour les paquets inférieurs à 512 octets. De plus ce co-processeur permet au module FortiGate-5002FB2 d'atteindre une performance proche des performances nominales de la ligne pour ces paquets. Les applications utilisant les petits paquets, telles que le protocole http et les mails, profiteront de cette accélération.

Les quatre autres ports servent aux applications utilisant des paquets de plus grandes tailles telles que les transferts FTP, les copies de fichiers et les accès basés serveurs.

Carte de Commutation FortiGate-5003

Tous les châssis FortiGate-5050 et FortiGate-5140 peuvent inclure jusqu'à deux modules FortiGate-5003.

Illustration 7 : Panneau avant du FortiGate-5003

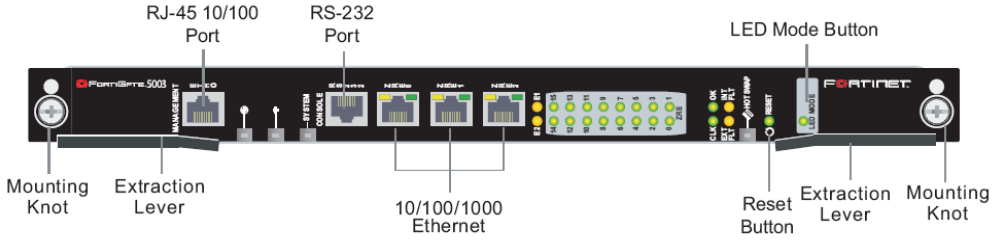


Tableau 9 : Les indicateurs des diodes électroluminescentes du module FortiGate-5003

Diode	État	Description
+	**Vert**	**Le module FortiGate-5003 est sous tension.**
	Jaune	**Sollicite la prudence. S'allume lorsqu'une des diodes CLOCK, OK ou INT FLT est défectueuse.**
	Jaune	**Hors service. La diode est généralement éteinte. Si allumée, présence d'une défaillance du commutateur.**
System Console	**Vert**	**Opère normalement.**
Port 0 - 15	**Jaune**	**Mode lien/activité – le port ne transfère pas de paquets.** **Mode lien/vitesse – indique une connexion de 1000 Mbit/s.**
	Vert	**Mode lien/activité – une diode clignotante indique un trafic réseau.** **Mode lien/vitesse – indique une connexion de 100 Mbit/s.**
	Eteint	**Mode lien/activité – pas de lien établi.** **Mode lien/vitesse – indique une connexion de 10 Mbit/s.**
E1	**Jaune**	**Mode lien/activité – le port ne transfère pas de paquets.** **Mode lien/vitesse – indique une connexion de 1000 Mbit/s.**
	Vert	**Mode lien/activité – une diode clignotante indique un trafic réseau.** **Mode lien/vitesse – indique une connexion de 100 Mbit/s.**
	Eteint	**Mode lien/activité – pas de lien établi.** **Mode lien/vitesse – indique une connexion de 10 Mbit/s.**
E0	**Jaune**	**Mode lien/activité – le port ne transfère pas de paquets.** **Mode lien/vitesse – indique une connexion de 1000 Mbit/s.**

Diode	État	Description
	Vert	**Mode lien/activité – une diode clignotante indique un trafic réseau.** **Mode lien/vitesse – indique une connexion de 100 Mbit/s.**
	Eteint	**Mode lien/activité – pas de lien établi.** **Mode lien/vitesse – indique une connexion de 10 Mbit/s.**
OK	**Vert**	**L'initialisation est terminée avec succès.**
EXT FLT	**Jaune**	**Ne peut pas établir un lien vers un port configuré ou présence d'un autre problème de connexion extérieur à l'adaptateur.**
INT FLT	**Jaune**	**Echec des tests internes. Eteint pendant la mise en route.**
Hot Swap	**Bleu**	**La diode allumée signifie que le commutateur est prêt à être retiré. Pendant un échange à chaud, la diode reste allumée. Elle s'éteint lorsque le commutateur est correctement installé.**
Reset		**Appuyer et maintenir la touche enfoncée pendant 3 secondes pour redémarrer le commutateur.**
LED Mode		**Passage de l'affichage des diodes des ports du mode Lien/Activité au mode Lien/Vitesse.**

Connexions

Les connexions interface suivantes sont disponibles sur le module FortiGate-5003.

Connecteur	Type	Vitesse	Protocole	Description
ETH0	**RJ-45**	**100Base-T**	**Ethernet**	**Connexion Ethernet de gestion hors bande**
CONSOLE	**RJ-45**	**9600 bit/s**	**Série RS-232**	**Connexion série vers l'interface de ligne de commande.**
ZRE0, ZRE1, ZRE2	**RJ-45**	**1000Base-T**	**Ethernet**	**Connexions redondantes vers un autre châssis FortiGate.**

Contrôleur de Gestionnaire de Châssis

Le module Contrôleur de Gestionnaire de Châssis FortiGate est responsable des mises en marche et à l'arrêt du châssis, ainsi que du traitement des ajouts et retraits de modules y compris la commutation des ressources interconnectées. De plus, il gère la distribution du courant, le processus de refroidissement et les statuts du châssis.

Illustration 8 : Panneau avant du Contrôleur de Gestionnaire de Châssis FortiGate 5050SM

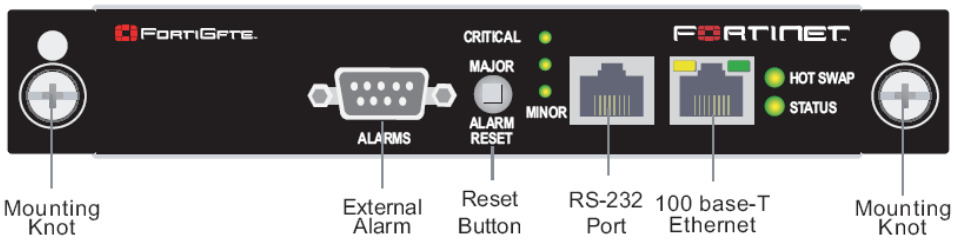

FortiGate
CRITICAL
MAJOR
MINOR
ALARMS
ALARM RESET
FORTINET
HOT SWAP
STATUS
Mounting Knot
External Alarm
Reset Button
RS-232 Port
100 base-T Ethernet
Mounting Knot

Illustration 9 : Panneau avant du Contrôleur de Gestionnaire de Châssis FortiGate 5140SM

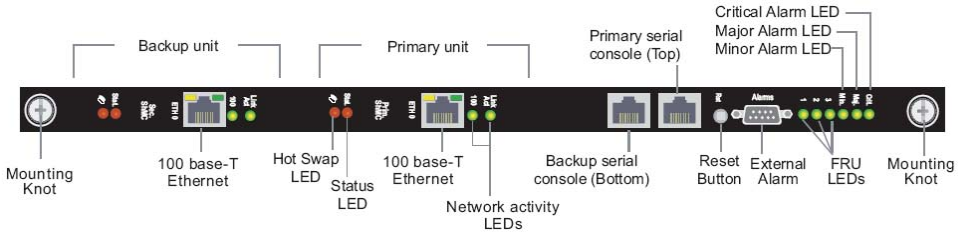


Tableau 10 : Les indicateurs des diodes électroluminescentes d'un module Gestionnaire de Châssis FortiGate

Diode	État	Description
MINOR CRITICAL MAJOR	**Vert**	**Opère normalement.**
	Rouge	**Indique le niveau d'alerte.**
HOT SWAP	**Bleu**	**La diode reste allumée pendant un échange à chaud.**
STATUS	**Vert**	**Opère normalement.**
Port Ethernet	**Jaune**	**Le port ne relaye pas les paquets.**
	Vert	**Une diode clignotante indique un trafic réseau.**
	Eteint	**Pas de lien établi.**

Connexions

Les connexions interface suivantes sont disponibles sur le module Gestionnaire de Châssis FortiGate.

Connecteur	Type	Vitesse	Protocole	Description
ALARMS	**DB-15**	**9600 bit/s**	**Série RS-232**	**L'interface d'alarme Telco à contacts secs (48VDC) fournit des connexions de type Telco form-c pour les problèmes mineurs, majeurs et critiques d'alimentation.**
Console	**RJ-45**	**9600 bit/s**	**Série RS-232**	**Connexion série pour l'interface de ligne de commande.**
Ethernet	**RJ-45**	**100Base-T**	**Ethernet**	**Fournit l'accès aux méthodes d'administration Telnet, Web ou SNMP.**

Contrôle du ventilateur et de la puissance

Les FortiGate-5140SM et FortiGate-5050SM contrôlent la température interne des châssis FortiGate. Si celle-ci dépasse un niveau acceptable, le gestionnaire de châssis FortiGate diminuera la puissance des cartes pare-feu antivirus pour réduire le niveau de chaleur. Le FortiGate-5140SM peut également augmenter la vitesse du ventilateur pour accélérer le refroidissement du châssis FortiGate-5140.

Contrôle du statut du châssis

Sur les modules FortiGate-5050SM et FortiGate-5140SM, le Gestionnaire de Châssis allume ou éteint un module FortiGate-5001 et négocie les ressources de courant de tous les modules.

Montage d'un châssis FortiGate série 5000

Remarque : Le châssis FortiGate doit être monté avant d'y installer les modules FortiGate série 5000.

Le châssis FortiGate doit être monté dans une armoire rack standard de 19 pouces. Vérifiez l'espace nécessaire pour chaque modèle :

- Châssis FortiGate-5020 4U
- Châssis FortiGate-5050 5U
- Châssis FortiGate-5140 12U

Si vous installez un équipement FortiGate dans un assemblage multi racks ou dans une armoire rack fermée, la température ambiante de l'armoire rack risque d'être plus élevée que la température ambiante de la pièce. Assurez-vous toujours que la température ambiante ne dépasse pas la température maximum indiquée par le constructeur.

Attention : Le châssis FortiGate ne doit pas fonctionner de manière isolée.

Circulation de l'air

Lors d'une installation dans une armoire rack, assurez-vous que la circulation d'air nécessaire au bon fonctionnement du FortiGate n'est pas compromise.

Installation d'un module FortiGate-500x

Toutes les procédures suivantes doivent être entièrement accomplies avant de pouvoir insérer un module FortiGate-500x dans le châssis FortiGate.

Installation des RAM DIMM

Le module FortiGate-500x est fourni avec deux RAM DIMM à insérer dans les slots RAM en haut du module FortiGate-500x. Il est nécessaire d'installer les RAM DIMM avant d'insérer le module FortiGate-500x dans le châssis FortiGate.

Installer les RAM DIMM FortiGate-500x

1. Déballez les RAM DIMM.
2. Installez-les dans les slots RAM en haut du module FortiGate-500x.
3. Les slots RAM ne permettent l'alignement que d'un module RAM DIMM. Si les leviers de verrouillage ne se ferment pas parfaitement cela signifie que votre DIMM n'est pas aligné correctement ou qu'il est à l'envers.
4. Poussez le RAM DIMM doucement jusqu'à ce que le mécanisme de verrouillage bloque le DIMM.
5. Répétez ces étapes pour les deux RAM DIMM.

Installation des transmetteurs SFP

Le FortiGate-500x est livré avec des transmetteurs 1000Base-SX SFP (fibre multimode) à insérer dans les emplacements du boîtier 1-4, dépendant du modèle du FortiGate. Les transmetteurs doivent être placés avant l'insertion du module FortiGate-500x dans le châssis FortiGate.

Remarque : Les transmetteurs SFP 1000Base-LX (fibre monomode) ou SFP 1000Base-TX (fibre cuivre) peuvent être utilisés facultativement. Les SX et LX nécessitent les transmetteurs fibre LC tandis que le TX nécessite l'emploi d'un connecteur RJ-45.

Installer les transmetteurs SFP FortiGate-500x

1. Otez les capuchons des emplacements SFP du panneau avant du FortiGate-500x.
2. En maintenant les côtés des transmetteurs SFP, glissez-les dans les emplacements jusqu'à ce qu'ils soient correctement positionnés.

Attention : Ne pas tenir les transmetteurs SFP par leur clenche de libération car cela pourrait endommager le connecteur.

Paramétrage des cavaliers

La carte FortiGate-5001 est pré-configurée avec les paramètres du cavalier pour le type de châssis auquel elle est destinée. Un des paramètres s'applique aux châssis qui possèdent un contrôleur de gestionnaire de châssis (FortiGate-5050 et FortiGate-5140). Un autre des paramètres s'applique aux châssis qui n'en possèdent pas (FortiGate-5020).

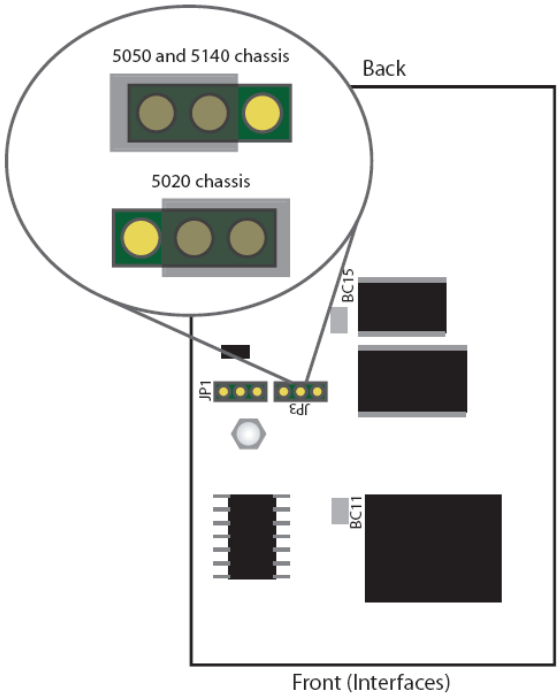
Le paramétrage du cavalier peut être erroné dans le cas où la pré-configuration est mauvaise. C'est aussi le cas si votre châssis a été mis à jour et est passé d'un FortiGate-5020 à un FortiGate-5050 ou FortiGate-5140. Dans tous les cas, il est nécessaire de modifier les paramètres du cavalier afin que la carte FortiGate-5001 puisse communiquer avec le Gestionnaire de Châssis.

Remarque : Cette procédure requiert un changement manuel des paramètres du cavalier sur la carte FortiGate-5001. Cela exige des connaissances suffisantes sur le sujet.

Modifier ou vérifier les cavaliers

1. Otez la carte FortiGate-5001 du châssis.
2. A partir du diagramme ci-dessous, localisez les paramètres du cavalier à main gauche de la carte lorsque le panneau avant (les ports des interfaces) vous fait face.
3. Retirez prudemment le cavalier et placez-le sur le paramètre correct.
4. Replacez la carte dans le châssis.

Illustration 10 : Les options du paramètre du cavalier



Installation d’un module FortiGate-500x

Les modules FortiGate-500x sont échangeables à chaud. Cela signifie que vous pouvez les retirer ou les installer alors que le châssis FortiGate est sous tension.

Remarque : Le levier d’extraction à gauche du panneau avant du FortiGate-500x est doté d’un commutateur caché. Ce levier doit être fermé pour que le module puisse recevoir le courant. Afin de s’assurer que ce levier reste fermé, les attaches de montage du module doivent être serrées après son insertion.

Installer un module FortiGate-500x

1. Assurez-vous que le module FortiGate-500x est à l'endroit et que les leviers d'extraction sont tendus.
2. En tenant le module FortiGate-500x par le panneau avant, glissez prudemment le module dans le slot du châssis. Veillez à glisser le module tout droit dans le slot. Utilisez le rail à l'intérieur du châssis pour guider le module jusqu'à ce qu'il touche le fond de panier du châssis FortiGate. Le module et le slot doivent être convenablement alignés et le module complètement et parfaitement positionné (le module touche alors le châssis jusqu'aux leviers d'extraction).
3. Verrouillez les leviers d'extraction en les poussant l'un vers l'autre pour vous assurer que le FortiGate-500x est bien en contact avec le fond de panier et placé en toute sécurité.

   Le module FortiGate-500x se met sous tension lorsque le châssis est sous tension et les leviers d'extraction fermés.
4. Serrez les attaches de montage des deux côtés du panneau avant du FortiGate-500x. Cela empêche les leviers d'extraction de s'ouvrir et de mettre le module FortiGate-500x hors tension.

Installation d'un module FortiGate-5003

Le module FortiGate-5003 est un module optionnel que vous pouvez installer dans les châssis FortiGate-5050 et FortiGate-5140.

L'utilisation du commutateur FortiGate-5003 nécessite l'installation du module dans les slots suivants :

- Pour un module FortiGate-5003, installez-le dans le slot 2.
- Pour deux modules FortiGate-5003, installez-les dans les slots 1 et 2.

Ces ports spécifiques sont câblés sur le fond de panier pour permettre des possibilités de commutation des ports internes, ainsi qu'une fonctionnalité HA. Si vous créez un cluster de modules pare-feu antivirus FortiGate-500x, l'installation d'un module FortiGate-5003 est indispensable.

Remarque : Le levier d'extraction à gauche du panneau avant du FortiGate-500x est doté d'un commutateur caché. Ce levier doit être fermé pour que le module puisse recevoir le courant. Afin de s'assurer que ce levier reste fermé, les attaches de montage du module doivent être serrées après son insertion.

Installer un module FortiGate-5003

1. Assurez-vous que le module FortiGate-5003 est à l'endroit et que les leviers d'extraction sont tendus.
2. En tenant le module FortiGate-5003 par le panneau avant, glissez prudemment le module dans le slot du châssis. Veillez à glisser le module tout droit dans le slot. Utilisez le rail à l'intérieur du châssis pour guider le module jusqu'à ce qu'il touche le fond de panier du châssis FortiGate. Le module et le slot doivent être convenablement alignés et le module complètement et parfaitement positionné (le module touche alors le châssis jusqu'aux leviers d'extraction).

3 Verrouillez les leviers d'extraction en les poussant l'un vers l'autre pour vous assurer que le FortiGate-5003 est bien en contact avec le fond de panier et placé en toute sécurité.

   Si le châssis est sous tension, le module FortiGate-5003 s'allume lorsque les leviers d'extraction sont fermés.

4 Serrez les attaches de montage des deux côtés du panneau avant du FortiGate-5003. Cela empêche les leviers d'extraction de s'ouvrir et de mettre le module FortiGate-5003 hors tension.

Installation du module Gestionnaire de Châssis FortiGate

Le module Gestionnaire de Châssis FortiGate est un module optionnel que vous pouvez installer dans les châssis FortiGate-5050 et FortiGate-5140. Le module Gestionnaire de Châssis 5050 s'installe dans le slot à main droite tout en bas du châssis FortiGate-5050. Le module Gestionnaire de Châssis 5140 s'installe dans le slot le plus à droite du châssis FortiGate-5140.

Installer le module Gestionnaire de Châssis FortiGate

1 Assurez-vous que le module Gestionnaire de Châssis FortiGate est à l'endroit.

2 En tenant le module par le panneau avant, glissez-le prudemment dans le slot du châssis.

   Veillez à glisser le module tout droit dans le slot. Utilisez le rail à l'intérieur du châssis pour guider le module jusqu'à ce qu'il touche le fond de panier du châssis FortiGate. Le module et le slot doivent être convenablement alignés et le module complètement et parfaitement positionné (le module touche alors le châssis).

3 Serrez les attaches de montage des deux côtés du panneau avant du Gestionnaire de Châssis FortiGate.

Mise en marche du Gestionnaire de Châssis

Lors de sa mise en marche, le Gestionnaire de Châssis démarre le logiciel. Les informations du démarrage sont accessibles via le port Série.

Pour visualiser les informations de démarrage et configurer les variables d'environnement, vous devez disposer :

- d'une connexion série entre le module Gestionnaire de Châssis FortiGate et l'ordinateur d'administration.
- d'un logiciel d'émulation terminal tel que l'HyperTerminal de Microsoft Windows sur l'ordinateur d'administration.

Lorsque le module s'allume, le message suivant s'affiche sur la console :

```
ARMboot 1.0.2 (Apr 18 2003 - 14:58:54)
   ARMboot code: 10f00000 -> 10f156a4
   DRAM Configuration:
   Bank #0: 10000000 16 MB
   Flash: 8 MB Hit any key to stop autoboot: 0
   ShMM #
```

Ajustement des variables d'environnement

Lors de l'installation du Gestionnaire de Châssis FortiGate, celui-ci démarre automatiquement. Etablissez les variables d'environnement pour le module.

Etablir l'environnement du démarrage

1. Connectez-vous en CLI au module Gestionnaire de Châssis FortiGate en utilisant une connexion série à l'ordinateur d'administration. Utilisez le logiciel d'émulation terminal (l'HyperTerminal de Microsoft Windows) sur l'ordinateur d'administration.
2. Etablissez les variables d'environnement reprises dans le tableau ci-dessous.
3. Pour affecter les valeurs aux variables d'environnement, entrez la commande suivante :

   ```
   clia setenv <variable_name> <new_value>
   ```

   Par exemple:

   ```
   clia setenv ipaddr 10.10.10.1
   ```

   Etablissez les variables d'environnement suivantes :

ipaddr	**Adresse IP utilisée par l'interface Ethernet.**
ipdevice	**Equipement repris dans ipaddr. Par défaut : « eth0 ».**
netmask	**Masque de réseau. Par défaut : 255.255.0.0**
hostname	**Nom du réseau.**
serverip	**Adresse IP du serveur TFTP.**

4. Pour régler l'horloge du module, entrez la commande suivante :

   ```
   clia date MMDDHHMMSSYYYY
   ```

   où
   - MM est le mois
   - DD est le jour
   - HH est l'heure
   - MM est la minute
   - SS est la seconde
   - YYYY est l'année

   Par exemple

   ```
   clia date 02151628002005
   ```

5. Entrez la commande suivante pour sauvegarder les paramètres d'environnement sur la mémoire Flash :

   ```
   clia saveenv
   ```

Connexion au Contrôleur de Gestionnaire de Châssis

Pour configurer le Contrôleur de Gestionnaire de Châssis, vous pouvez vous connecter via les entrées sur le panneau avant du module.

Deux méthodes permettent la configuration du Contrôleur de Gestionnaire de Châssis :

- L'interface de ligne de commande via le port RS-232 ou Telnet via le port Ethernet.
- L'interface d'administration web connectée au port Ethernet via un navigateur web.

Ces deux méthodes vous informent sur le statut des modules, la configuration des capteurs d'informations, les paramètres seuils et les statuts généraux.

Commandes CLI du Contrôleur de Gestionnaire de Châssis

Les commandes CLI suivantes sont utiles pour obtenir des informations à partir de votre Gestionnaire de Châssis FortiGate. Pour obtenir une liste complète des commandes, tapez `help` dans l'interface de ligne de commande. Pour entrer le mode de commande du Gestionnaire de Châssis, tapez `clia` avant chaque commande. Par exemple :

```
clia getfanlevel
```

Tableau 11 : Commandes CLI de Gestionnaire de Châssis

Commande	Syntaxe	Description
alarm	**alarm [clear |minor | major | critical]**	**Fournit un accès vers les sorties d'alarme TELCO. Les paramètres « minor », « major » et « critical » vous permettent de choisir l'alarme correspondante. Ces actions sont cumulatives.**
fans	**fans [-v] [<IPMBaddress> [<FRU-device-ID>]]**	**Affiche les informations sur le ventilateur FRU spécifié. Cette commande affiche aussi les informations suivantes :** • **Adresse IPMB et ID de l'équipement FRU** • **Niveau de vitesse minimum** • **Niveau de vitesse maximum** • **Niveau de vitesse continue maximum** • **Niveau en cours (les niveaux "contrôle local » et « ignorer » si les deux sont disponibles.)**
getfanlevel	**getfanlevel <IPMBaddress> <FRU-device-ID>**	**Affiche le niveau de vitesse du ventilateur en cours.**
setfanlevel	**setfanlevel <IPMBaddress>**	**Règle le nouveau niveau de vitesse du ventilateur.** Disponible uniquement

Commande	Syntaxe	Description
	<IPMBaddress> <FRU-device-ID> <level>	**du ventilateur.** Disponible uniquement sur le FortiGate-5140SM.
Getthreshold **threshold**	**getthreshold board <N> [<sensor-name> | <sensor-number>]]**	**Affiche les valeurs des seuils en cours. Le capteur doit être un capteur basé sur les seuils. Les valeurs brutes et traitées sont affichées. Les données suivantes s'affichent également :** **• Adresse IPMB du contrôleur IPM propriétaire.** **• Numéro du capteur, nom du capteur (chaîne d'identification provenant du SDR) et le numéro logique à partir duquel le capteur peut être atteint.** **• Le type de capteur et le code de lecture du type d'évènement.**
setthreshold	**setthreshold <IPMBaddress> <sensor-name> <threshold-type> [-r] <value>**	**Modifie la valeur en cours du seuil pour le seuil spécifié du capteur spécifié. Le capteur est spécifié par l'adresse IPMB du contrôleur IPM propriétaire et par le nom ou numéro du capteur. Le capteur cible doit être un capteur basé sur les seuils. Le paramètre <threshold-type> peut être spécifié comme l'une des valeurs symboliques suivantes:** **• "upper_non_recoverable" (pouvant être abrégé par "unr")** **• "upper_critical" (pouvant être abrégé par "uc")** **• "upper_non_critical" (pouvant être abrégé par "unc")** **• "lower_non_recoverable" (pouvant être abrégé par "lnr")** **• "lower_critical" (pouvant être abrégé par "lc")** **• "lower_non_critical" pouvant être abrégé par "lnc")** **Par défaut, la valeur cible est spécifiée selon son unité (par exemple, en volts pour les capteurs de voltage ou en degrés Celsius pour les capteurs de température). L'option –r signifie qu'une valeur brute est utilisée à la place d'une unité.**
shelf	**shelf <subcommand>** **cooling_state** **fans_state**	**Fournit des informations clés et des données sélectionnées sur le fonctionnement en cours du Châssis.**

Commande	Syntaxe	Description
	power_distribution **power_management** **MaxCurrent [feed]** **<Amps>** **MinVoltage [feed]** **<Volts>**	

Alimentation du châssis

Chaque équipement FortiGate fonctionne selon ses propres exigences en matière de courant électrique. Celles-ci sont reprises ci-dessous. Veillez à ce que les fiches de connexions adaptées soient correctement mises en place avant de brancher le courant sur les châssis FortiGate.

Le châssis FortiGate pourrait surcharger votre circuit d'alimentation et impacter votre protection de surcourant et le câblage d'alimentation. Utilisez un étiquetage approprié pour solliciter la prudence.

Châssis FortiGate-5020

Deux fiches de connexion au dos du châssis FortiGate-5020 fournissent du courant alternatif aux alimentations de courant. Chacune des fiches de connexion doit être connectée à une source de courant différente. De cette manière, si une source tombe en panne, l'autre source reste opérationnelle.

Attention : Le châssis FortiGate-5020 se présente avec deux modules d'entrée d'alimentation de courant redondants 120 – 240 volts alternatifs et un module de sorties 48 volts continus. Ces modules se trouvent sur le châssis derrière le panneau d'alimentation amovible.

Mettre le châssis FortiGate-5020 sous tension

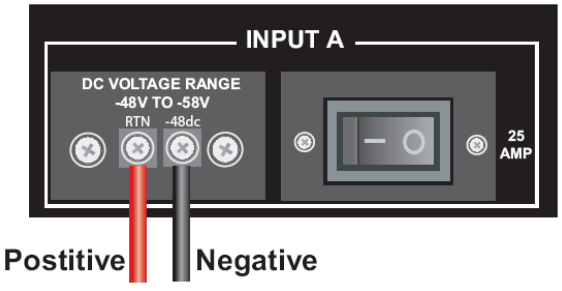
1. Assurez-vous que les interrupteurs au dos du châssis sont fermés.
2. Connectez les câbles aux fiches de connexion au dos du châssis.
3. Connectez les câbles aux prises de courant.
4. Ouvrir les interrupteurs.

   Les diodes de courant s'allument lorsque le courant est connecté et fonctionne correctement.

Châssis FortiGate-5050

Le châssis FortiGate-5050 possède deux fiches de connexion d'alimentation de courant redondantes 48 – 58 volts continus à l'arrière du châssis.

Deux fiches de connexion au dos du châssis FortiGate-5050 fournissent du courant continu aux alimentations de courant. Chacune des fiches de connexion doit être connectée à une source de courant différente. De cette manière, si une source tombe en panne, l'autre source reste opérationnelle.



Dans le cas où le courant continu est indisponible, vous pouvez installer le module de conversion d'alimentation FortiGate-5053 pour convertir une alimentation de courant alternatif en courant continu.

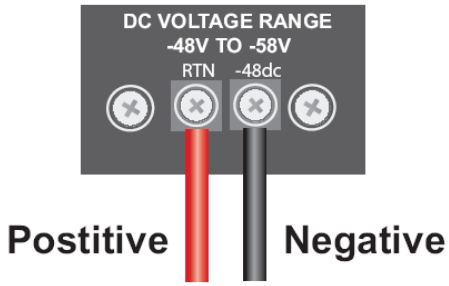
Mettre le châssis FortiGate-5050 sous tension

1. Assurez-vous que les interrupteurs du châssis et de la source de courant sont fermés.
2. Connectez le câble électrique négatif (noir) à la vis de fin (Neg) -48dc.
3. Connectez le câble électrique positif (rouge) à la vis de fin RTN (Pos)
4. Ouvrez la source de courant et l'interrupteur du châssis.

Châssis FortiGate-5140

Le châssis FortiGate-5140 possède deux fiches de connexion d'alimentation de courant redondantes 48 – 58 volts continus à l'arrière du châssis.

Deux fiches de connexion au dos du châssis FortiGate-5140 fournissent du courant continu aux alimentations de courant. Chacune des fiches de connexion doit être connectée à une source de courant différente. De cette manière, si une source tombe en panne, l'autre source reste opérationnelle.



Dans le cas où le courant continu est indisponible, vous pouvez installer le le module de conversion d'alimentation FortiGate-5053 pour convertir une alimentation de courant alternatif en courant continu.

Mettre le châssis FortiGate-5140 sous tension

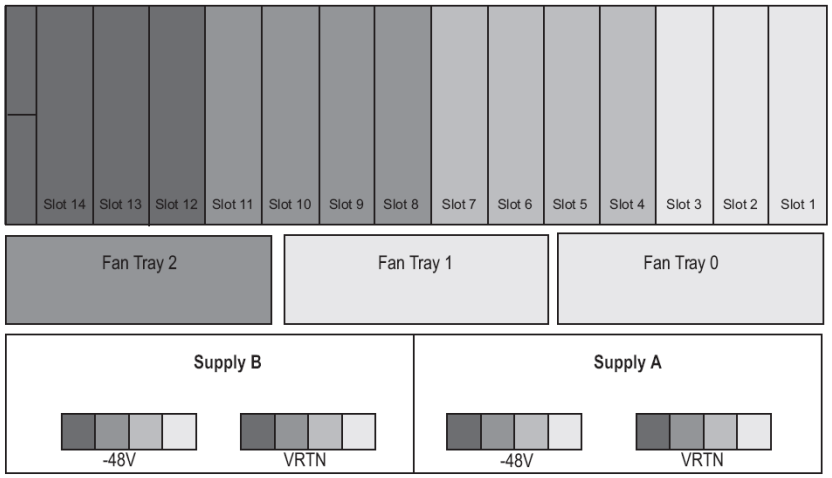
1. Assurez-vous que les interrupteurs du châssis et de la source de courant soient fermés.
2. Connectez le câble électrique négatif (noir) à la vis de fin (Neg) -48dc.
3. Connectez le câble électrique positif (rouge) à la vis de fin RTN (Pos)
4. Ouvrez la source de courant et l'interrupteur du châssis.

Distribution de courant via le FortiGate-5140

Le châssis Fortigate-5140 permet l'option de diviser le système en quatre zones de courant. Chacune de ces zones fournit un courant redondant à une section séparée du fond de panier.

L'illustration suivante représente le panneau arrière du châssis et la distribution de courant pour chaque alimentation.

Illustration 11 : Alimentations de courant sur un FortiGate-5140



Module d'alimentation AC du châssis

Dans le cas où il serait nécessaire de fournir aux châssis FortiGate-5050 et FortiGate-5140 du courant alternatif, le module de Conversion d'Alimentation FortiGate-5053 peut convertir le courant continu en courant alternatif.

Illustration 12 : Le module de Conversion d'Alimentation FortiGate-5053

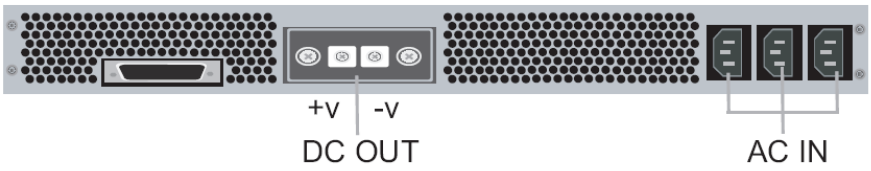
Le module de conversion d'alimentation FortiGate-5053 supporte jusqu'à trois modules d'alimentation de courant échangeables à chaud, ce qui offre une fiabilité et un temps de disponibilité sans point unique de panne. Pour plus de détails sur ces modules échangeables à chaud, voir « Modules d'alimentation de courant échangeables à chaud » à la page 49. Le module d'alimentation AC du châssis peut être installé au-dessus ou au-dessous du châssis FortiGate.

Remarque : Un minimum de deux alimentations de courant est requis pour faire fonctionner le module.

Connexion du module de Conversion d'Alimentation au châssis FortiGate

Chaque module de conversion d'alimentation fournit une source de courant alternatif redondante pour les châssis FortiGate-5050 et FortiGate-5140 équipés d'une entrée de courant continu. Utilisez deux modules FortiGate-5053 comme alimentations de courant redondantes.

Illustration 13 : Panneau arrière du module de Conversion d'Alimentation FortiGate-5053



Connecter le module de conversion d'alimentation au châssis FortiGate

1. Eteignez le courant du châssis. Pour plus de détails sur la mise hors tension, voir « Mise en service du châssis » à la page 40.
2. Connectez les câbles de courant alternatif aux fiches de connexions au dos du châssis FortiGate.
3. Connectez les câbles de courant alternatif aux prises de courant. Connectez les fiches de connexion de courant alternatif à différentes sources de courant. De cette manière si une des sources tombe en panne, l'autre reste opérationnelle.
4. Connectez les alimentations de courant continu aux connexions finales du module de conversion d'alimentation.
5. Connectez les alimentations de courant continu aux connexions finales au dos du châssis FortiGate, tel que décrit dans la section « Mise en service du châssis » à la page 40.

   Veillez à éteindre le système d'exploitation FortiGate avant d'éteindre l'interrupteur du châssis, ceci afin d'éviter tout dysfonctionnement.

Mettre le châssis FortiGate hors tension

1. - A partir de l'interface d'administration web, sélectionnez **Système > Maintenance > Eteindre**. Sélectionnez Eteindre et cliquez sur Appliquer.

   - A partir de l'interface de ligne de commande, entrez :

   ```
   execute shutdown
   ```
2. Fermez l'interrupteur.
3. Fermez les deux interrupteurs.
4. Déconnectez l'alimentation de courant.
5. Déconnectez le câble de l'alimentation.

Connexion du FortiGate

Deux méthodes permettent la connexion et la configuration des paramètres de base du FortiGate :

- L'interface d'administration web
- L'interface de ligne de commande (CLI)

Interface d'administration web

Vous pouvez configurer et gérer le FortiGate avec une connexion HTTP ou HTTPS, à partir de tout ordinateur muni de Microsoft Internet Explorer 6.0 ou de tout autre navigateur récent. L'interface d'administration web fonctionne en plusieurs langues.

L'interface d'administration web permet la configuration et la gestion de la plupart des paramètres FortiGate.

Interface de ligne de commande (CLI)

Vous pouvez accéder à l'interface de ligne de commande FortiGate en connectant le port série de votre ordinateur au port console du FortiGate. Vous pouvez également avoir recours à Telnet ou à une connexion sécurisée SSH pour vous connecter en CLI à partir de n'importe quel réseau connecté au FortiGate, y compris Internet.

Accès à l'interface d'administration web

La procédure suivante retrace les étapes pour une première connexion à l'interface d'administration web. Les changements de configuration apportés via l'interface d'administration web sont instantanément pris en compte, sans qu'il soit nécessaire de réinitialiser le pare-feu et sans interruption de service.

Pour vous connecter à l'interface d'administration web, vous devez disposer :

- d'un ordinateur avec une connexion Ethernet
- de Microsoft Internet Explorer version 6.0 ou plus ; ou toute récente version de navigateur web
- d'un câble Ethernet croisé ou d'un concentrateur ou commutateur Ethernet et deux câbles Ethernet

Remarque : Avant de démarrer Internet Explorer, vérifier sur votre FortiGate que la connexion physique entre l'ordinateur et le FortiGate fonctionne correctement.

Connexion à l’interface d’administration web

Se connecter à l’interface d’administration web à partir de l’interface interne

1. Configurez votre ordinateur avec l’adresse IP statique 192.168.1.2 et le masque de réseau 255.255.255.0.
2. Connectez l’interface interne de l’équipement FortiGate au réseau fibre.
3. Connectez l’interface de votre ordinateur au même réseau.
4. Démarrez Internet Explorer et entrez l’adresse https://192.168.1.99 (n’oubliez pas d’inclure le « s » dans https://).

   Pour assurer une méthode sécurisée d’authentification HTTPS, le FortiGate dispose d'un certificat de sécurité auto-signé, et il lui est envoyé aux clients distants à chaque fois qu’ils initient une connexion HTTPS vers le FortiGate. Lors de l’établissement de la connexion, le FortiGate affiche deux alertes dans la fenêtre du navigateur.

   La première alerte vous demande d’accepter et d’installer, à titre facultatif, le certificat de sécurité auto-signé FortiGate. Si vous refusez ce certificat, le FortiGate refuse la connexion. Si vous l’acceptez, la page d’ouverture de la session du FortiGate s’affiche. Les informations de connexion (compte administrateur et mot de passe) sont chiffrées avant d’être envoyées au FortiGate. Si vous choisissez d’accepter le certificat de manière permanente, l’alerte n’apparaîtra plus.

   Juste avant l’affichage de la page d’ouverture de la session, une deuxième alerte vous informe que le nom du certificat FortiGate diffère de celui de la demande originale. Cette alerte se produit car le FortiGate redirige la connexion. C’est un message informatif. Sélectionnez OK pour continuer l’ouverture de la session.

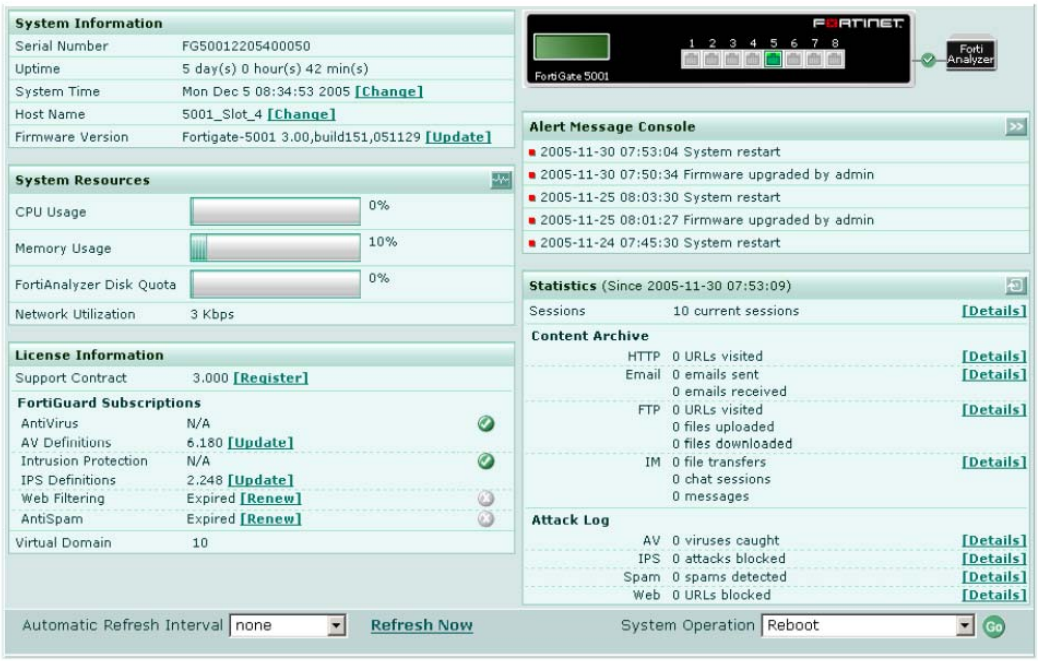
   Illustration 14 : Ouverture d'une session sur le FortiGate

5. Tapez `admin` dans le champ Nom et cliquez sur Login.

Tableau de bord du système

Une fois la connexion à l'interface d'administration web établie, la fenêtre de navigation affiche le tableau de bord du système qui reprend tous les statuts du système.

Illustration 15 : Tableau de bord du système FortiGate-5001



Le tableau de bord reprend les informations suivantes :

- Statut des Ports (Port Status) – le tableau de bord affiche la face avant du FortiGate, ainsi que le statut de la connexion au FortiAnalyser - un X indiquant une absence de connexion, un V la présence de connexion. En plaçant le curseur de la souris sur un des ports, les informations suivantes sur son statut s'affichent:
  - le statut du port (up ou down)
  - l'adresse IP et le masque de réseau
  - la vitesse et le nombre total de paquets envoyés et reçus

  Chaque port actif apparaît en vert.
- Information système (System Information) – regroupe les informations sur le système d'exploitation telles que le numéro de série de l'équipement et la version de code. Cette zone vous permet de mettre à jour le logiciel, de programmer la date et l'heure et de changer de mode de fonctionnement.
- Ressources du système (System Resources) – permet de surveiller l'utilisation des ressources du FortiGate.
- Statut des licences (License Information) – affiche les mises à jour actuelles des antivirus et des systèmes de sécurité de votre FortiGate.
- Console de Messages d'Alerte (Alert Message Console) - affiche les messages d'alerte des événements récents.
- Statistiques (Statistics) – fournit les informations statistiques en temps réel sur le trafic et les attaques.

Connexion à partir de l’interface de ligne de commande

Comme alternative à l’interface graphique, vous pouvez installer et configurer le FortiGate à partir de l’interface de ligne de commande. Les changements apportés dans la configuration à partir de l’interface de ligne de commande sont instantanément pris en compte, sans qu’il soit nécessaire de réinitialiser le pare-feu et sans interruption de service.

Pour vous connecter en CLI au FortiGate, vous devez disposer:

- d’un ordinateur avec un port de communication disponible
- du câble null-modem inclus parmi le matériel livré
- d’un logiciel d’émulation terminal tel que l'HyperTerminal de Microsoft Windows

Remarque : La procédure suivante s’appuie sur le logiciel Microsoft Windows HyperTerminal. Vous pouvez appliquer la même procédure avec tout programme d’émulation terminal.

Se connecter en CLI :

1. Connectez votre câble null-modem au port de communication (port série) de votre ordinateur d’une part et au port de la console du FortiGate d’autre part.
2. Démarrez le logiciel HyperTerminal, entrez un nom pour la connexion et cliquez sur OK.
3. Configurez l'HyperTerminal afin de vous connecter directement au port de communication de votre ordinateur et cliquez sur OK.
4. Sélectionnez les paramètres suivants du port et cliquez ensuite sur OK :

Bits par seconde	9600
Bits de données	8
Parité	Aucune
Bits d'arrêt	1
Contrôle de flux	Aucun

5. Appuyez sur la touche Enter pour vous connecter en CLI au FortiGate. Le message d’ouverture de la session apparaît.
6. Tapez `admin` et appuyez deux fois sur la touche Enter.

   Le message suivant s’affiche :

   ```
   Welcome !
   ```

   Tapez ? pour afficher les commandes disponibles. Pour plus d’informations à propos de l’utilisation de l’interface de ligne de commande, reportez-vous au *Guide de Référence CLI.*

Remplacement des modules

Dans le cas où l'un des modules devait tomber en panne ou être remplacé, il est aisé de les changer, les châssis FortiGate série 5000 supportant l'échangeabilité à chaud de modules. Vous pouvez donc retirer un module FortiGate défaillant et le remplacer par un nouveau tout en maintenant le châssis FortiGate opérationnel.

Echangeabilité à chaud de modules FortiGate-500x

Remarque : Le levier d'extraction à gauche du panneau avant du FortiGate-500x est doté d'un commutateur caché. Ce levier doit être fermé pour que le module puisse recevoir le courant. Afin de s'assurer que ce levier reste fermé, les attaches de montage du module doivent être serrées après son insertion.

Echanger à chaud des modules FortiGate-500x

1. Desserrez les trois vis de verrouillage et dégagez l'interrupteur intégré avant de continuer.
2. Desserrez les deux attaches de montage qui maintiennent le module dans le châssis et dévisser la vis du levier d'extraction de la carte sur le côté gauche. Ne pas retirer les attaches de montage.
3. Tout en maintenant le module FortiGate-500x par son panneau avant, tirez les leviers d'extraction jusqu'à ce que la diode IPM commence à clignoter et attendez un moment.
4. Lorsque la diode IPM reste allumée, utilisez les leviers d'extraction pour glisser le module en dehors du châssis.
5. En tenant le nouveau module FortiGate-500x par le panneau avant, glissez prudemment le module dans le slot du châssis.

   Veillez à glisser le module tout droit dans le slot. Utilisez le rail à l'intérieur du châssis pour guider le module jusqu'à ce que celui-ci touche le fond de panier du châssis FortiGate. Le module et le slot doivent être convenablement alignés et le module complètement et parfaitement positionné (le module touche alors le châssis jusqu'aux leviers d'extraction).
6. Verrouillez les leviers d'extraction en les poussant l'un vers l'autre pour vous assurer que le FortiGate-500x est bien en contact avec le fond de panier et placé en toute sécurité.

   Si le châssis est sous tension, le module FortiGate-500x s'allume lorsque les leviers d'extraction sont fermés.
7. Serrez les attaches de montage des côtés droit et gauche du panneau avant du FortiGate-500x. Cela empêche les leviers d'extraction de s'ouvrir et de mettre le module FortiGate-500x hors tension.

Modules d’alimentation de courant échangeables à chaud

Echangeabilité à chaud signifie que vous pouvez retirer un module d’alimentation de courant défaillant et le remplacer par un nouveau tout en maintenant le châssis FortiGate opérationnel.

Echanger à chaud des modules d’alimentation de courant

1. Fermez l’interrupteur du module d’alimentation de courant à remplacer avant de retirer le panneau d’alimentation amovible.
2. Retirez le panneau d’alimentation de l’avant du châssis FortiGate en desserrant les attaches de montage du panneau d’alimentation.
3. Desserrez les deux attaches de montage qui maintiennent le module dans le châssis. Ne pas retirer les attaches de montage.
4. Tout en maintenant le module d’alimentation de courant par sa poignée, glissez le module en dehors du châssis.
5. En tenant le nouveau module par sa poignée, glissez-le prudemment dans le slot vide du châssis.
6. Utilisez le rail à l’intérieur du châssis pour guider le module jusqu’à ce que celui-ci touche le fond de panier du châssis FortiGate.
7. Serrez les attaches de montage sur le module d’alimentation de courant.
8. Replacez le panneau d’alimentation amovible.
9. Ouvrez l’interrupteur du nouveau module d’alimentation de courant.

Paramétrage par défaut

Le module antivirus pare-feu FortiGate-500x vous est fourni avec une configuration par défaut qui vous permet de vous connecter à l'interface d'administration web et de configurer l'accès du module au réseau. Pour cela, vous devez entrer un mot de passe administrateur, modifier les adresses IP de l'interface du réseau, compléter les adresses IP du serveur DNS, et, si nécessaire, configurer le routage de base.

Si vous pensez utiliser votre module antivirus pare-feu FortiGate-500x en mode Transparent, commencer d'abord par changer le mode de fonctionnement pour ensuite configurer l'accès du module au réseau.

Une fois le paramétrage réseau terminé, vous pourrez configurer d'autres paramètres, comme les date et heure, la mise à jour des bases de connaissance antivirus et IPS, et procéder à l'enregistrement du FortiGate.

La configuration par défaut de votre pare-feu comprend une seule règle NAT (Network Address Translation) qui permet aux utilisateurs du réseau interne de se connecter au réseau externe et empêche les utilisateurs du réseau externe de se connecter au réseau interne. Vous pouvez étendre vos règles pare-feu en vue de contrôler davantage le trafic du réseau passant par le FortiGate.

Les profils de protection par défaut servent à la mise en place de différents niveaux de sécurité (antivirus, filtrage de contenu, filtrage antispam, et prévention d'intrusion) du trafic contrôlé par les règles pare-feu.

Ce chapitre couvre les sujets suivants :

- Configuration réseau en mode NAT/Route
- Configuration réseau en mode Transparent
- Configuration par défaut du pare-feu
- Profils de protection par défaut

Configuration réseau en mode NAT/Route

Lorsque le FortiGate est mis sous tension pour la première fois, il fonctionne en mode routé (NAT/Route) avec une configuration réseau par défaut telle que détaillée dans le tableau 12 ci-dessous. Cette configuration vous permet d'utiliser l'interface graphique du FortiGate et d'établir la configuration requise pour connecter le module antivirus pare-feu FortiGate-500x au réseau. Dans ce même tableau les droits d'administration HTTPS signifient que vous pouvez vous connecter à l'interface graphique en utilisant le protocole HTTPS. Lorsque la commande ping est spécifiée dans les droits d'accès, cela signifie que cette interface répond aux requêtes ping.

Tableau 12 : Configuration réseau par défaut en mode NAT/Route

Compte administrateur	**Nom de l'utilisateur :** **Mot de passe :**	**admin** **(néant)**
Port 1	**IP :** **Masque de réseau :** **Droits d'administration :**	**192.168.1.99** **255.255.255.0** **HTTPS, Ping**
Port 2	**IP :** **Masque de réseau :** **Droits d'administration :**	**192.168.100.99** **255.255.255.0** **Ping**
Port 3	**IP :** **Masque de réseau :** **Droits d'administration :**	**0.0.0.0** **0.0.0.0** **Ping**
Port 4	**IP :** **Masque de réseau :** **Droits d'administration :**	**0.0.0.0** **0.0.0.0** **Ping**
Port 5	**IP :** **Masque de réseau :** **Droits d'administration :**	**0.0.0.0** **0.0.0.0** **Ping**
Port 6	**IP :** **Masque de réseau :** **Droits d'administration :**	**0.0.0.0** **0.0.0.0** **Ping**
Port 7 (uniquement pour le FortiGate-5001)	**IP :** **Masque de réseau :** **Droits d'administration :**	**0.0.0.0** **0.0.0.0** **Ping**
Port 8 (uniquement pour le FortiGate-5001)	**IP :** **Masque de réseau :** **Droits d'administration :**	**0.0.0.0** **0.0.0.0** **Ping**
Paramètres du réseau	**Passerelle par défaut (pour route par défaut)**	**192.168.100.1**
	Interface connectée au réseau externe (pour route par défaut)	**port2**
	Route par défaut **Une route par défaut est constituée d'une passerelle par défau et de l'interface connectée au réseau extérieur (Internet généralement). Ces paramètres dirigent tout le trafic non local vers cette interface et le réseau externe.**	
	DNS primaire	**65.39.139.53**
	DNS secondaire	**65.39.139.63**

Configuration réseau en mode Transparent

En mode Transparent, le module antivirus pare-feu FortiGate-500x fonctionne avec une configuration réseau telle que détaillée dans le tableau 13 ci-dessous.

Tableau 13 : Configuration réseau par défaut en mode Transparent

Compte administrateur	**Nom d'utilisateur :** **Mot de passe :**	**admin** **(néant)**
Gestion IP	**IP :** **Masque de réseau :**	**0.0.0.0** **0.0.0.0**
DNS	**Serveur DNS primaire :** **Serveur DNS secondaire :**	**65.39.139.53** **65.39.139.63**
Droits d'administration	**Port 1** **Port 2** **Port 3** **Port 4** **Port 5** **Port 6** **Port 7 (uniquement pour le FortiGate-5001)** **Port 8(uniquement pour le FortiGate-5001)**	**HTTPS, Ping** **Ping** **Ping** **Ping** **Ping** **Ping** **Ping** **Ping**

Configuration par défaut du pare-feu

Les règles pare-feu du module antivirus pare-feu FortiGate-500x contrôlent l'accès ou le rejet des flux réseau par celui-ci. Tant qu'aucune règle n'est définie, aucun trafic n'est accepté par le FortiGate. Reportez-vous au *Guide d'Administration FortiGate* pour plus d'informations sur l'ajout de règles pare-feu.

Les paramètres suivants sont pré-configurés dans la configuration par défaut afin de faciliter l'ajout de règles pare-feu.

Tableau 14 : Configuration par défaut du pare-feu

Paramètres de configuration	Nom	Description
Adresse	**All**	**Représente toute valeur d'adresse réseau.**
Service	**Plus de 50 services prédéfinis**	**Sélectionnez les services désirés parmi les 50 services prédéfinis pour contrôler le trafic reçu.**
Plage horaire	**Toujours (Always)**	**Une plage récurrente est valable à tout moment.**
Profil de Protection	**Strict, scan, web, unfiltered**	**Définit quels sont les services de sécurité additionnels qui doivent être appliqués au flux: antivirus, filtrage web antispam, et IPS.**

La configuration par défaut du pare-feu est la même dans les modes NAT/Route et Transparent.

Profils de protection par défaut

Vous pouvez définir plusieurs profils de protection auxquels vous appliquez des niveaux de protection différenciés du trafic contrôlé par le FortiGate. Vous pouvez utiliser des profils de protection pour :

- appliquer un contrôle antivirus aux règles HTTP, FTP, IMAP, POP3 et SMTP
- activer du filtrage Web statique sur les règles HTTP
- appliquer du filtrage web dynamique, par catégorie, sur ces mêmes règles HTTP
- activer les services antispam sur les règles IMAP, POP3 et SMTP
- activer les services de prévention d'intrusion sur tous les flux
- activer la journalisation de contenu pour les flux HTTP, FTP, IMAP, POP3 et SMTP

Les profils de protection permettent la création de plusieurs types de protection qui vont s'appliquer à différentes règles pare-feu.
Par exemple, alors que le trafic entre des zones interne et externe nécessite une protection stricte, le trafic entre zones de confiance internes peut n'avoir besoin que d'une protection modérée. Vous pouvez configurer des règles pare-feu dans le but d'utiliser des profils de protection identiques ou différents selon les flux.

Des profils de protection sont disponibles en mode routé et transparent.

Quatre profils de protection sont pré-configurés:

Strict	Applique une protection maximum pour le trafic HTTP, FTP, IMAP, POP3 et SMTP. Vous n'utiliserez probablement pas ce profil rigoureux de protection en circonstances normales mais il est disponible en cas de problème de virus nécessitant une analyse maximum.
Scan	Applique une analyse antivirus et une mise en quarantaine de fichiers du contenu du trafic HTTP, FTP, IMAP, POP3 et SMTP. La mise en quarantaine est également applicable à tous les trafics. Sur les modèles FortiGate possédant un disque dur, la détection d'un virus entraîne le placement du fichier infecté en quarantaine sur le disque local du FortiGate. Si nécessaire, les administrateurs peuvent rétablir les fichiers en quarantaine.
Web	Applique une analyse antivirus et un blocage du contenu web. Vous pouvez ajouter ce profil de protection aux règles pare-feu qui contrôlent le trafic HTTP.
Unfiltered (Non filtré)	N'applique ni analyse, ni blocage, ni IPS. A utiliser dans le cas où aucune protection du contenu du trafic n'est souhaitée. Vous pouvez ajouter ce profil de protection aux règles pare-feu pour les connexions entre des réseaux hautement fiables et sécurisés dont le contenu ne nécessite pas d'être protégé.

Restauration du paramétrage par défaut

Si vous avez fait une erreur de configuration et que vous n'arrivez pas à connecter le module antivirus pare-feu FortiGate-500x, vous pouvez toujours restaurer les paramètres par défaut et recommencer la configuration.

Attention : Cette procédure supprime tous les changements apportés à la configuration du FortiGate et rétablit les paramètres par défaut, y compris ceux des interfaces, comme les adresses IP.

Restauration du paramétrage par défaut à partir de l’interface d’administration web

Pour rétablir les paramètres par défaut

1. Allez dans **Système > Statut > System Operation**.
2. Sélectionnez Réinitialiser aux paramètres par défaut.
3. Cliquez sur Go.

Restauration du paramétrage par défaut à partir de l’interface de ligne de commande

Pour rétablir les paramètres par défaut

Pour rétablir les paramètres par défaut, utilisez la commande suivante :

```
execute factoryreset
```

Configuration du FortiGate pour sa mise en réseau

Cette section vous donne un aperçu des modes de fonctionnement du FortiGate. Avant de procéder à la configuration du FortiGate, il est important de planifier la manière dont vous allez l'intégrer sur le réseau. La planification de la configuration dépend du mode de fonctionnement sélectionné : le mode NAT/Route ou le mode Transparent.

Cette section traite les sujets suivants:

- Planification de la configuration du FortiGate
- Installation en mode NAT/Route
- Installation en mode Transparent
- Étapes suivantes

Planification de la configuration du FortiGate

Avant de procéder à la configuration du FortiGate, il est nécessaire de planifier l'intégration du FortiGate au réseau, et de décider, notamment :

- de la visibilité de votre équipement sur le réseau
- des fonctions pare-feu à fournir
- du contrôle à appliquer au trafic

La planification de la configuration dépend du mode de fonctionnement sélectionné: le mode NAT/Route (par défaut) ou le mode Transparent.

Vous pouvez également configurer le FortiGate et le réseau qu'il protège en gardant le paramétrage par défaut.

Mode NAT/Route

En mode routé, le FortiGate est visible sur le réseau. De même que pour un routeur, ses interfaces sont présentes sur différents sous-réseaux.

Dans ce mode, les interfaces suivantes de la carte FortiGate-5001 sont disponibles :

- Les ports 1 à 4 peuvent être connectés à n'importe quel réseau Ethernet optique.
- Les ports 5 à 8 peuvent être connectés à n'importe quel réseau Ethernet cuivre.

En mode routé, les interfaces suivantes de la carte FortiGate-5002A sont disponibles :

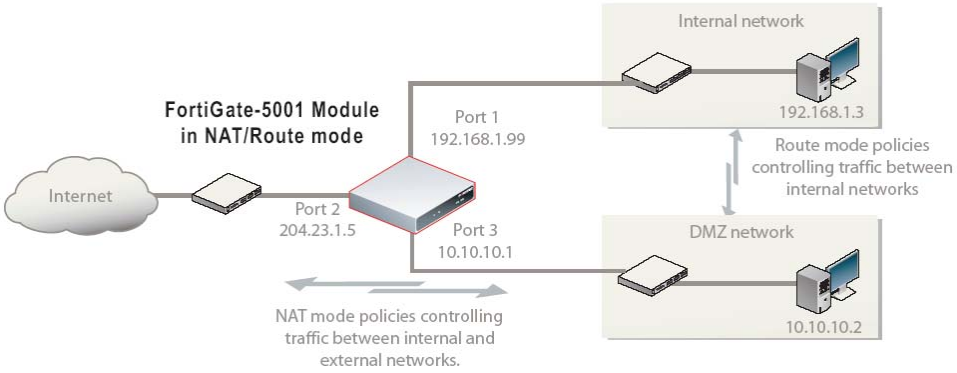
- Les ports 1 et 2 peuvent être connectés à n'importe quel réseau Ethernet fibre.
- Les ports 3 à 6 peuvent être connectés à n'importe quel réseau Ethernet cuivre.

Vous pouvez ajouter des règles pare-feu pour vérifier si le FortiGate opère en mode NAT ou en mode Route. Ces règles contrôlent la circulation du trafic en se basant sur les adresses sources et de destination, ainsi que sur les protocoles et ports applicatifs de chaque paquet. En mode NAT, le FortiGate exécute une translation des adresses du réseau avant d'envoyer le paquet vers le réseau de destination. En mode Transparent, il n'y a pas de translation d'adresses.

Le mode NAT/Route est généralement utilisé lorsque le FortiGate opère en tant que passerelle entre réseaux privés et publics. Dans cette configuration, vous pouvez activer de la translation d'adresse au niveau des règles pare-feu qui contrôlent le trafic circulant entre les réseaux interne et externe (généralement Internet).

Remarque : Vous pouvez créer des règles pare-feu en mode route pour gérer le trafic circulant entre plusieurs réseaux internes, par exemple entre une zone démilitarisée et votre réseau interne.

Illustration 16 : Exemple de configuration réseau d'une carte FortiGate-5001 en mode NAT/Route



Mode NAT/Route avec de multiples connexions externes

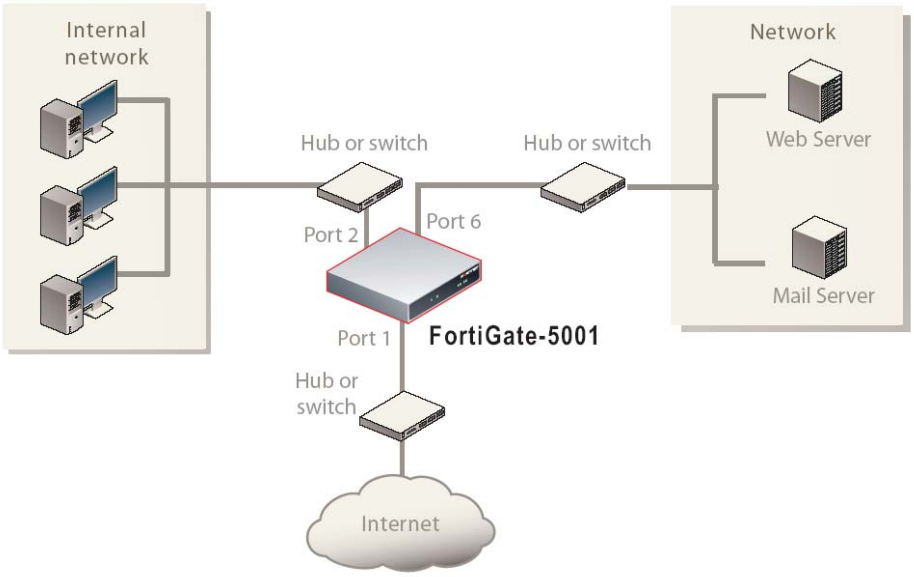
En mode routé, le FortiGate peut se configurer avec des connexions multiples et redondantes au réseau externe.
Vous pourriez, par exemple, créer la configuration suivante :

- Le port 2 pour l'interface par défaut du réseau externe (généralement Internet)
- Le port 1 pour l'interface du réseau interne
- Le port 6 pour l'interface d'un autre réseau interne

Votre configuration doit permettre au routage de supporter des connexions Internet redondantes. Le routage peut automatiquement rediriger les connexions d'une interface dans le cas où la connexion au réseau externe échoue.

Par ailleurs, la configuration de règles de sécurité est la même que pour une configuration en mode routé avec une seule connexion Internet. Vous établirez des règles pare-feu en mode NAT pour contrôler le trafic circulant entre les réseaux interne et externe.

Illustration 17 : Exemple de configuration de multiples connexions Internet en mode NAT/Route



Mode Transparent

En mode Transparent, le FortiGate n'est pas visible sur le réseau. De même que pour un pont, toutes ses interfaces doivent se trouver sur le même sous-réseau. Il suffit de configurer une adresse IP d'administration pour pouvoir procéder à des modifications dans la configuration et la mise à jour des bases de connaissance antivirus et IPS.

Le mode Transparent d'un FortiGate est généralement utilisé sur un réseau privé derrière un pare-feu ou un routeur existant. Le FortiGate exécute les fonctions de pare-feu, VPN IPSec, analyse de virus, protection d'intrusion et filtrage web et antispam.
Vous pouvez connecter le FortiGate afin de contrôler le trafic échangé entre ces segments réseaux:

- Le port 1 peut se connecter au pare-feu ou routeur externe.
- Tous les autres ports peuvent se connecter à d'autres segments réseau.

Installation en mode NAT/Route

Cette section décrit l'installation du FortiGate en mode NAT/Route.

Cette section couvre les sujets suivants:

- Préparation de la configuration du FortiGate en mode NAT/Route
- Configuration DHCP ou PPPoE
- A partir de l'interface d'administration web
- A partir de l'interface de ligne de commande
- Connexion du FortiGate au(x) réseau(x)
- Configuration des réseaux

Préparation de la configuration du FortiGate en mode NAT/Route

Vous pouvez consigner les informations nécessaires à la personnalisation des paramètres du mode NAT/Route dans le tableau 15 à la page suivante.

Vous pouvez configurer le FortiGate de deux manières :

- A partir de l'interface d'administration web GUI qui est une interface complète pour configurer la plupart des paramètres. Voir « A partir de l'interface d'administration web » à la page 60.
- A partir de l'interface de ligne de commande (CLI) qui est une interface textuelle complète pour configurer tous les paramètres. Voir « A partir de l'interface de ligne de commande» à la page 62.

Le choix de la méthode dépend de la complexité de la configuration et des types d'accès, d'équipement et d'interface qui vous sont les plus familiers.

Tableau 15 : Paramètres du mode NAT/Route

Mot de passe administrateur**:**		
Port 1	**IP :** **Masque de réseau :**	_____._____._____._____ _____._____._____._____
Port 2	**IP :** **Masque de réseau :**	_____._____._____._____ _____._____._____._____
Port 3	**IP :** **Masque de réseau :**	_____._____._____._____ _____._____._____._____
Port 4	**IP :** **Masque de réseau :**	_____._____._____._____ _____._____._____._____
Port 5	**IP :** **Masque de réseau :**	_____._____._____._____ _____._____._____._____
Port 6	**IP :** **Masque de réseau :**	_____._____._____._____ _____._____._____._____
Port 7 (FortiGate-5001 et FortiGate-5001FA2)	**IP :** **Masque de réseau :**	_____._____._____._____ _____._____._____._____
Port 8 (FortiGate-5001 et FortiGate-5001FA2)	**IP :** **Masque de réseau :**	_____._____._____._____ _____._____._____._____
Paramètres du réseau	**Passerelle par défaut :**	_____._____._____._____
	Interface connectée au réseau externe (Port 2 généralement)	
	Une route par défaut est constituée d'une passerelle par défaut et de l'interface connectée au réseau externe (Internet généralement). Ces paramètres dirigent tout le trafic non local vers cette interface et le réseau externe.	
	Serveur DNS primaire : **Serveur DNS secondaire :**	_____._____._____._____ _____._____._____._____

Configuration DHCP ou PPPoE

Les interfaces du FortiGate peuvent acquérir leur adresse IP depuis un serveur DHCP ou PPPoE. Votre fournisseur d'accès Internet peut vous fournir des adresses IP via l'un de ces protocoles.

Pour utiliser le serveur FortiGate DHCP, il vous faut configurer pour ce serveur une plage intervalle d'adresses IP et une route par défaut. Ce protocole ne nécessite pas d'autres informations de configuration.

Le protocole PPPoE nécessite, quant à lui, un nom d'utilisateur et un mot de passe. De plus, les configurations non numérotées PPPoE requièrent une adresse IP. Servez-vous du tableau 16 ci-dessous pour consigner les informations nécessaires à la configuration PPPoE.

Tableau 16 : Paramètres PPPoE

Nom d'utilisateur :	
Mot de passe :	

A partir de l’interface d’administration web

Vous pouvez utiliser l’interface graphique pour la configuration initiale du FortiGate et de tous ses paramètres.

Pour plus d’informations sur l’accès à l’interface d’administration web, voir « Accès à l’interface d’administration web » à la page 44.

Configuration des paramètres de base

Après vous être connecté à l’interface d’administration web, vous pouvez utiliser les procédures suivantes pour compléter la configuration de base de votre FortiGate.

Ajouter/modifier le mot de passe administrateur

1. Sélectionnez **Système > Admin > Administrateurs.**
2. Cliquez sur l’icône Changer le mot de passe pour l’administrateur admin.
3. Entrez un nouveau mot de passe et entrez-le une seconde fois pour confirmation.
4. Cliquez sur OK.

Configurer les interfaces

1. Sélectionnez **Système > Réseau > Interface.**
2. Cliquez sur l’icône Editer d’une des interfaces.
3. Choisissez un mode d’adressage : manuel, DHCP ou PPPoE.
4. Complétez la configuration d’adressage.
   - Pour un adressage manuel, entrez l’adresse IP et le masque de réseau de l’interface.
   - Pour un adressage DHCP, sélectionnez DHCP et tous les paramètres requis.
   - Pour un adressage PPPoE, sélectionnez PPPoE et entrez compte utilisateur, mot de passe et autres paramètres requis.

   Pour plus d’informations sur la configuration des paramètres des interfaces, consultez l’aide en ligne FortiGate ou le *Guide d’Administration FortiGate.*
5. Cliquez sur OK.

Répétez cette procédure pour chaque interface.

Remarque : Si vous modifiez l’adresse IP de l’interface à laquelle vous êtes connecté, vous devez vous reconnecter à partir d’un navigateur web avec la nouvelle adresse. Connectez-vous à https:// suivi de la nouvelle adresse IP de l’interface. Si la nouvelle adresse IP de l’interface est sur un sous-réseau différent, vous devrez probablement modifier l’adresse IP de votre ordinateur et la configurer sur le même sous-réseau.

Configurer les paramètres du serveur DNS

1. Sélectionnez **Système > Réseau > Options.**
2. Entrez l’adresse IP du serveur DNS primaire.

3 Entrez l’adresse IP du serveur DNS secondaire.

4 Cliquez sur Appliquer.

Ajout d’une route par défaut

Ajouter une route par défaut permet de configurer la destination vers laquelle le FortiGate enverra le trafic destiné au réseau externe (Internet généralement). Cela sert également à définir l’interface connectée au réseau externe. La route par défaut n’est pas requise si cette interface est connectée en DHCP ou PPPoE.

Ajouter une route par défaut

1 Sélectionnez **Routage > Route Statique.**

2 Si le tableau de Route statique stipule une route par défaut (IP et masque configurés à 0.0.0.0), cliquez sur l’icône Suppression pour effacer cette route.

3 Sélectionnez Créer nouveau.

4 Affectez l’adresse IP destination 0.0.0.0.

5 Affectez le Masque 0.0.0.0.

6 Configurez l’adresse IP de la passerelle par défaut dans le champ Passerelle.

7 Affectez Device à l’interface connectée au réseau externe.

8 Cliquez sur OK.

Vérification de la configuration à partir de l’interface d’administration web

Pour vérifier les paramètres d’accès, cliquez sur l’interface que vous voulez vérifier et sélectionnez l’icône Editer. Les paramètres sélectionnés lors de la procédure précédente doivent apparaître cochés dans le champ des droits d’administration.

Tester la connexion

La procédure suivante permet de tester la connexion:

- Consultez le site www.fortinet.com
- Importez ou envoyez un courrier électronique de votre boîte aux lettres.

Si vous ne parvenez pas à vous connecter au site web, à importer ou envoyer un courrier électronique, vérifiez la procédure précédente point par point pour vous assurer que toutes les informations ont été entrées correctement. Puis recommencez le test.

A partir de l’interface de ligne de commande

Vous pouvez également configurer votre FortiGate en utilisant les commandes CLI. Pour toute information sur la connexion en CLI, voir « Connexion à partir de l’interface de ligne de commande » à la page 47.

Configuration du FortiGate pour opérer en mode NAT/Route

Reportez-vous aux informations consignées dans le tableau 15 de la page 59 pour accomplir la procédure suivante.

Ajouter/modifier le mot de passe administrateur

1. Connectez-vous en CLI.
2. Pour modifier le mot de passe administrateur admin. Tapez :

```
config system admin
   edit admin
      set password <psswrd>
  end
```

Configurer les interfaces

1. Connectez-vous en CLI.
2. Affectez à l’interface interne l’adresse IP et le masque de réseau tels que consignés au tableau 15 de la page 59. Tapez :

```
config system interface
   edit internal
      set mode static
      set ip <address_ip> <netmask>
  end
```

Exemple

```
config system interface
   edit internal
      set mode static
      set ip 192.168.120.99 255.255.255.0
  end
```

3. Affectez à l’interface externe l’adresse IP et le masque de réseau tels que consignés au tableau 15 de la page 59. Tapez :

```
config system external
   edit external
      set mode static
      set ip <address_ip> <netmask>
  end
```

Exemple

```
config system external
   edit external
      set mode static
      set ip <204.28.1.5> <255.255.255.0>
  end
```

Configurer dynamiquement l’interface externe par DHCP

```
config system interface
   edit external
      set mode dhcp
  end
```

Configurer dynamiquement l’interface externe par PPPoE

```
config system interface
   edit external
      set mode pppoe
      set connection enable
      set username <name_str>
      set password <psswrd>
  end
```

4 Utilisez la même syntaxe pour affecter une adresse IP à chaque interface.

5 Confirmez que les adresses sont correctes. Entrez :

```
get system interface
```

L’interface CLI énumère les adresses IP, masques de réseau et autres paramètres pour chaque port du FortiGate.

Configurer les paramètres du serveur DNS

Configurer les serveurs DNS primaire et secondaire :

```
config system dns
      set primary <address_ip>
      set secondary <address_ip>
  end
```

Exemple

```
config system dns
      set primary 293.44.75.21
      set secondary 293.44.75.22
  end
```

Ajout d’une route par défaut

Ajouter une route par défaut permet de configurer la destination vers laquelle le FortiGate enverra le trafic destiné au réseau externe (Internet généralement). Cela sert également à définir l’interface connectée au réseau externe. La route par défaut n’est pas requise si cette interface est connectée en DHCP ou PPPoE.

Ajouter une route par défaut

Définissez l’adresse IP de la Passerelle par défaut :

```
config router static
     edit 1
      set dst 0.0.0.0 0.0.0.0
      set gateway <gateway_IP>
      set device <interface>
  end
```

Exemple

Si l'IP de la passerelle par défaut est 204.23.1.2 et que celle-ci est connectée au WAN1 :

```
config router static
    edit 1
      set dst 0.0.0.0 0.0.0.0
      set gateway 204.23.1.2
      set device wan1
  end
```

Vérification de la configuration à partir de l'interface de ligne de commande

Pour vérifier les paramètres d'accès, entrez la commande CLI suivante :

```
show system interface
```

Le programme d'émulation terminal devrait afficher les interfaces, vdom, adresses IP, droits d'administration, et paramètres-types du FortiGate.

Exemple :

```
   edit internal
      set vdom "root"
      set ip 192.168.1.99 255.255.255.0
      set allowaccess ping https ssh snmp http
      set type physical
```

Tester la connexion

La procédure suivante permet de tester la connexion:

- Lancez un ping à destination du FortiGate.
- Connectez-vous à l'interface graphique GUI.
- Importez ou envoyez un courrier électronique de votre boîte aux lettres.

Si vous ne parvenez pas à vous connecter au site web ou à importer ou envoyer un courrier électronique, vérifiez la procédure précédente point par point pour vous assurer que toutes les informations entrées sont correctes. Puis recommencez le test.

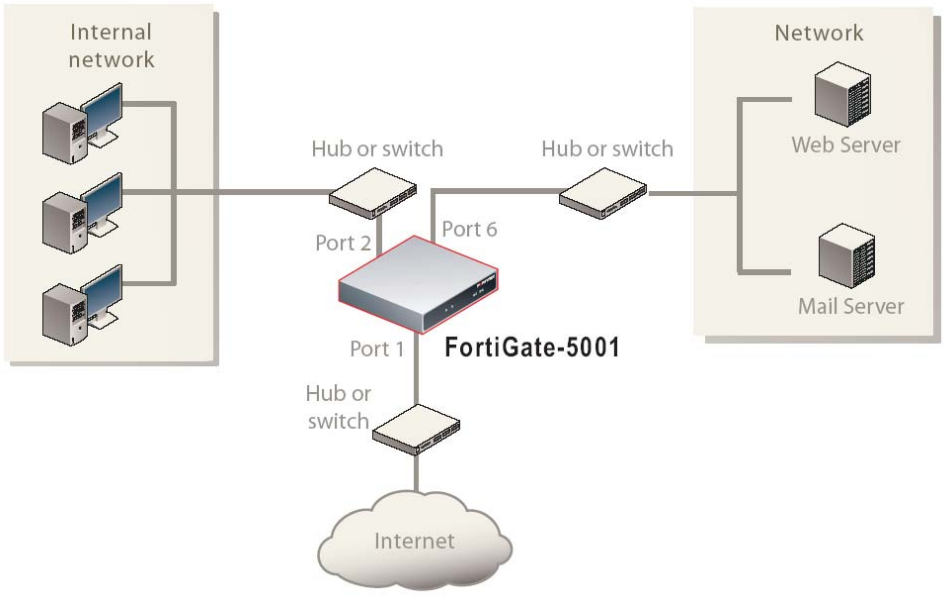
Connexion du FortiGate au(x) réseau(x)

Une fois la configuration initiale terminée, vous pouvez connecter le FortiGate entre le réseau interne et Internet.

Pour le module FortiGate-5001 : Connectez les interfaces 1 à 4 à des réseaux gigabits Ethernet fibre optique et les interfaces 5 à 8 à des réseaux gigabits Ethernet cuivre.

Pour le module FortiGate-5002 : Connectez les interfaces 1 à 6 à des réseaux gigabits Ethernet cuivre.

Illustration 18 : Connexions du FortiGate-5001 en mode NAT/Route



Configuration des réseaux

En mode routé, vos réseaux doivent être configurés de manière à diriger tout le trafic Internet vers l'adresse IP de l'interface où les réseaux sont connectés.

Si vous utilisez le module antivirus pare-feu FortiGate-500x comme serveur DHCP pour votre réseau interne, configurez les ordinateurs de votre réseau interne conformément au protocole DHCP.

Assurez-vous que votre module antivirus pare-feu FortiGate-500x fonctionne correctement en vous connectant à Internet à partir d'un ordinateur de votre réseau interne. Vous devriez pouvoir accéder à n'importe quelle adresse Internet.

Installation en mode Transparent

Cette section décrit l'installation du FortiGate en mode Transparent.

Cette section couvre les sujets suivants:

- Préparation de la configuration du FortiGate en mode Transparent
- A partir de l'interface d'administration web
- A partir de l'interface de ligne de commande
- Connexion du FortiGate à votre réseau

Préparation de la configuration du FortiGate en mode Transparent

Reportez-vous au tableau 17 ci-dessous pour consigner les informations nécessaires à la personnalisation des paramètres du mode Transparent.

Deux méthodes permettent la configuration du mode Transparent :

- L'interface d'administration web GUI
- L'interface de ligne de commande (CLI)

Le choix de la méthode dépend de la complexité de la configuration et du type d'accès, d'équipement et d'interface qui vous sont les plus familiers.

Tableau 17 : Paramètres du mode Transparent

Mot de passe Administrateur **:**		
IP d'administration	**IP :** **Masque de réseau :** **Passerelle par défaut :**	_____._____._____._____ _____._____._____._____ _____._____._____._____
	L'adresse IP et le masque de réseau configurés pour l'administration du FortiGate doivent être accessibles dep le réseau à partir duquel vous allez gérer le FortiGate. Ajoutez une passerelle par défaut si le poste d'administra et le FortiGate ne sont par sur le même sous-réseau.	
Paramétrage DNS	**Serveur DNS primaire :** **Serveur DNS secondaire :**	_____._____._____._____ _____._____._____._____

A partir de l'interface d'administration web

Vous pouvez utiliser l'interface d'administration web pour compléter la configuration initiale du FortiGate et de tous ses paramètres.

Pour plus d'informations sur l'accès à l'interface d'administration web, voir « Accès à l'interface d'administration web » à la page 44. La première connexion au FortiGate se fait en mode NAT/Route.

Passer en mode Transparent à partir de l'interface d'administration web

1. Sélectionnez **Système > Statut**.
2. Cliquez sur Changer à côté du champ Mode de fonctionnement.
3. Sélectionnez Transparent dans la liste Operation Mode.

   Entrez l'adresse IP/Masque de réseau d'administration et l'adresse de la Passerelle par défaut consignées dans le tableau 17 à la page 66.
4. Cliquez sur Appliquer.

Il n'est pas nécessaire de se reconnecter à l'interface d'administration web, les changements sont immédiatement pris en compte en cliquant sur Appliquer. Vous pouvez vérifier le passage en mode Transparent sur le tableau de bord du FortiGate.

Configurer les paramètres du serveur DNS

1. Sélectionnez **Système > Réseau > Options**.
2. Entrez l'adresse IP du serveur DNS primaire.
3. Entrez l'adresse IP du serveur DNS secondaire.
4. Cliquez sur Appliquer.

A partir de l’interface de ligne de commande

Comme alternative à l’interface graphique, vous pouvez commencer la configuration initiale du FortiGate via les commandes CLI. Pour se connecter en CLI, voir « Connexion à partir de l’interface de ligne de commande » à la page 47. Reportez-vous aux informations consignées dans le tableau 17 de la page 66 pour accomplir les procédures suivantes.

Passer en mode Transparent à partir de l’interface de ligne de commande

1. Assurez-vous d’être connecté en CLI
2. Pour passer en mode Transparent, entrez :

```
config system settings
      set opmode transparent
      set manageip <address_ip> <netmask>
      set gateway <address_gateway>
   end
```

Après quelques secondes, le message suivant s’affiche :

```
Changing to TP mode
```

3. Lorsque le message d’ouverture de la session s’affiche, entrez :

```
get system settings
```

Le CLI affiche le statut du FortiGate notamment l’adresse IP et le masque de réseau d’administration :

```
opmode        : transparent
manageip      : <address_ip><netmask>
```

Assurez-vous de l’exactitude des paramètres du serveur DNS. Ceux-ci étant importés du mode NAT/Route, ils risquent d’être erronés pour la configuration en mode Transparent. Reportez-vous au tableau 17 de la page 66 pour paramétrer le serveur DNS.

Vérifier le paramétrage du serveur DNS

Entrez la commande suivante pour vérifier le paramétrage du serveur DNS FortiGate :

```
show system dns
```

Cette commande CLI donne les informations suivantes:

```
config system dns
     set primary 293.44.75.21
     set secondary 293.44.75.22
     set fwdintf internal
   end
```

Configurer les paramètres du serveur DNS

Affectez les adresses IP des serveurs DNS primaire et secondaire. Entrez :

```
config system dns
     set primary <address_ip>
     set secondary <address_ip>
   end
```

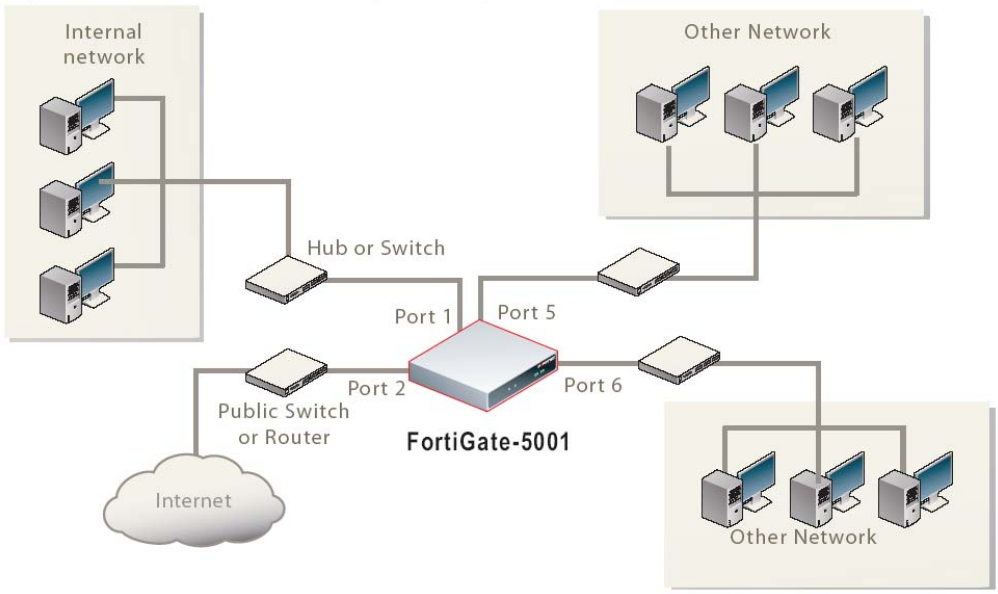
Connexion du module FortiGate à votre réseau

Une fois la configuration initiale terminée, vous pouvez connecter le module antivirus pare-feu FortiGate-500x à votre réseau.

Pour le module FortiGate-5001 : Connectez les interfaces 1 à 4 à des réseaux gigabits Ethernet fibre optique et les interfaces 5 à 8 à des réseaux gigabits Ethernet cuivre.

Pour le module FortiGate-5002 : Connectez les interfaces 1 à 6 à des réseaux gigabits Ethernet cuivre.

Illustration 19 : Connexions du FortiGate-5001 en mode Transparent



Tester la connexion

La procédure suivante permet de tester la connexion:

- Lancez un ping à destination du FortiGate.
- Connectez-vous à l'interface d'administration web GUI.
- Consultez ou envoyez un courrier électronique de votre boîte aux lettres.

Si vous ne parvenez pas à vous connecter au site web ou à consulter/envoyer un courrier électronique, vérifiez la procédure précédente point par point pour vous assurer que toutes les informations entrées sont correctes. Puis, recommencez le test.

Étapes suivantes

Les instructions suivantes vous permettront de paramétrer la date et l'heure, d'enregistrer le FortiGate et de configurer la mise à jour des bases de connaissance antivirus et IPS.

Reportez-vous au *Guide d'Administration FortiGate* pour obtenir des informations détaillées sur la configuration, le contrôle et la maintenance du FortiGate.

Paramétrage des date et heure

Il est important que la date et l'heure du système du FortiGate soient exactes. Le paramétrage peut se faire soit manuellement, soit automatiquement en configurant le FortiGate pour qu'il se synchronise avec un serveur NTP (Network Time Protocol).

Paramétrer la date et l'heure

1. Sélectionnez **Système > Statut**.
2. Dans **Statut > Heure système**, cliquez sur Changer.
3. Sélectionnez Actualiser pour afficher les date et heure actuelles du système.
4. Sélectionnez votre fuseau horaire dans la liste.
5. Cochez éventuellement « Ajuster automatiquement lors du passage à l'heure d'été / l'heure d'hiver ».
6. Sélectionnez Réglage et réglez la date et l'heure exactes.
7. Réglez heure, minute, seconde, année, mois et jour.
8. Cliquez sur OK.

Remarque : Si vous avez sélectionné l'option « Ajuster automatiquement lors du passage à l'heure d'été / l'heure d'hiver » l'ajustement des date et heure lors du retour à l'heure d'hiver doit se faire manuellement.

Synchronisation des date et heure avec un serveur NTP

1. Sélectionnez **Système > Statut.**
2. Dans **Statut > Heure système**, sélectionnez Changer.
3. Sélectionnez Synchroniser avec le serveur NTP pour un paramétrage automatique des date et heure.
4. Entrez l'adresse IP ou le nom de domaine d'un serveur NTP que le système utilisera pour régler la date et l'heure.
5. Spécifiez l'intervalle de synchronisation.
6. Cliquez sur OK.

Enregistrement de votre FortiGate

Après avoir installé un nouvel équipement FortiGate, enregistrez celui-ci sur le site http://support.fortinet.com en cliquant sur « Product Registration ».

Afin de procéder à l'enregistrement, entrez vos coordonnées et le(s) numéro(s) de série de(s) nouveau(x) équipement(s) FortiGate acquis. Plusieurs enregistrements peuvent être introduits lors d'une seule session.

L'enregistrement des nouveaux équipements vous permet d'accéder aux supports techniques et aux mises à jour des bases de données de détection et prévention contre des menaces (Antivirus, Détection d'Intrusion, etc.).

Mise à jour des signatures antivirus et IPS

Vous pouvez configurer le FortiGate pour qu'il se connecte au FortiGuard Distribution Network (FDN – Réseau de Distribution FortiGuard), et mette à jour les bases de connaissance des antivirus, antispam et attaques IPS.

Le FDN est un réseau mondial de FortiGuard Distribution Servers (FDS – Serveurs de Distribution FortiGuard). En se connectant au FDN, le FortiGate se relie au FDS le plus proche grâce à sa liste d'adresses préprogrammées triées en fonction du fuseau horaire sélectionné.

La mise à jour des signatures antivirus et IPS peut se faire soit via l'interface graphique, soit via l'interface de ligne de commande. Pour accéder aux mises à jour votre équipement FortiGate doit avant tout être enregistré. Pour plus d'informations sur l'enregistrement de votre FortiGate, voir « Enregistrement de votre FortiGate » à la page 70.

Remarque : Il est fortement conseillé de mettre les signatures antivirus et IPS régulièrement à jour afin d'éviter que votre FortiGate ne devienne vulnérable face aux nouveaux virus.

Après avoir procédé à l'enregistrement, vérifiez la connexion entre le FortiGate et le FDN :

- Les date et heure doivent être exactes.
- À partir de l'interface d'administration web, sélectionnez « Réactualiser » dans le Centre FortiGuard (FortiGuard Center).

Si la connexion au FDN échoue, recommencez la procédure d'enregistrement de votre FortiGate ou reportez-vous à « Ajout d'un serveur override » à la page 73.

Mise à jour des signatures antivirus et IPS à partir de l'interface d'administration web

Une fois votre équipement FortiGate enregistré, vous pouvez mettre les signatures antivirus et IPS à jour à partir de l'interface d'administration web. Le Centre FortiGuard permet de recevoir des mises à jour par courrier électronique. Pour ce faire, entrez une adresse IP pour la réception de ces courriers et programmez une fréquence de mise à jour hebdomadaire, quotidienne, voire à chaque heure.

Mettre les signatures antivirus et IPS à jour

1. Sélectionnez **Système > Maintenance > FortiGuard Center**.
2. Sélectionnez Mettre à jour.

   En cas de succès de connexion au FDN, l'interface d'administration web affiche le message suivant :

   ```
   "Your update request has been sent. Your database will be
   updated in a few minutes. Please check your update page for
   the status of the update."
   ```

   A savoir:
   ```
   Votre demande de mise à jour a été envoyée. Votre base de
   données va être mise à jour dans quelques minutes. Merci de
   vérifier le statut de la mise à jour sur la page mise à jour.
   ```

   Lorsqu'une mise à jour est disponible, la page du Centre FortiGuard listera, après quelques minutes, les nouvelles versions d'antivirus, en fonction de leurs dates de création et numéros de version. Le journal Evénement enregistre les messages témoignant du succès ou de l'échec des mises à jour.

Remarque : La mise à jour des définitions d'antivirus, par l'ajout de nouvelles signatures par FortiGate dans la base de données, peut entraîner une brève rupture du trafic analysé. Il est dès lors préférable de programmer les mises à jour lorsque le trafic est faible, par exemple pendant la nuit.

Mise à jour des signatures IPS à partir de l'interface de ligne de commande

Il est possible de mettre les signatures IPS à jour en utilisant des commandes CLI ci-dessous.

Remarque : La mise à jour des signatures antivirus ne peut se faire qu'à partir de l'interface d'administration web.

Mettre les signatures IPS à jour à partir de l'interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante :

   ```
   configure system autoupdate ips
      set accept-recommended-settings enable
      end
   ```

Programmation des mises à jour des signatures antivirus et IPS

Il est possible de planifier une programmation régulière et automatique des mises à jour des signatures antivirus et IPS, soit via l'interface d'administration web, soit via l'interface de ligne de commande.

Activer la programmation de mises à jour à partir de l'interface d'administration web

1. Sélectionnez **Système > Maintenance > FortiGuard Center.**
2. Cochez la case Programmation des mises à jour régulières.
3. Sélectionnez une des fréquences suivantes pour la vérification et le téléchargement des mises à jour :

Chaque	La mise à jour a lieu selon un intervalle de temps prédéfini. Sélectionnez le temps souhaité (nombre d'heures, entre 1 et 23 heures) entre chaque demande de mise à jour.
Journalière	La mise à jour a lieu quotidiennement. Vous pouvez en spécifier l'heure précise dans la journée.
Hebdomadaire	La mise à jour a lieu une fois par semaine. Vous pouvez en spécifier le jour et l'heure.

4. Cliquez sur Appliquer.

La nouvelle programmation de fréquence entre en vigueur immédiatement.

A chaque fois que le FortiGate procède à une mise à jour, l'action est enregistrée dans le journal Evénement.

Activer la programmation de mises à jour à partir de l'interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante :

```
config system autoupdate schedule
      set day
      set frequency
      set status
      set time
   end
```

Exemple :

```
config system autoupdate schedule
      set update every Sunday
      set frequency weekly
      set status enable
      set time 16:45
   end
```

Ajout d’un serveur override

Dans le cas où vous ne parvenez pas à vous connecter au FDN, ou encore si votre entreprise vous fournit les mises à jour de leur propre serveur FortiGuard, les procédures suivantes vous permettront d’ajouter une adresse IP d’un serveur override FortiGuard soit via l’interface graphique, soit via l’interface de ligne de commande.

Ajouter un serveur override à partir de l’interface d’administration web

1. Sélectionnez **Système > Maintenance > FortiGuard Center**.
2. Cochez la case Utiliser l’adresse de remplacement.
3. Entrez le nom de domaine entier ou l’adresse IP d’un serveur FortiGuard.
4. Cliquez sur Appliquer.

Le FortiGate teste la connexion vers le serveur override.
En cas de succès, le paramètre du FDN affiche un statut disponible.
Dans le cas contraire où le FDN affiche un statut de service indisponible, le FortiGate n’arrivant pas à se connecter au serveur override, vérifiez les configurations du FortiGate et du réseau et tentez de déceler les paramètres empêchant la connexion au serveur override FortiGuard.

Ajouter un serveur override à partir de l’interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante :

```
config system autoupdate override
      set address
      set status
   end
```

Logiciel FortiGate

Fortinet met régulièrement le logiciel FortiGate à jour en y intégrant des améliorations et résolutions aux problèmes d'adresses. Une fois votre module antivirus pare-feu FortiGate-500x enregistré, le logiciel peut être téléchargé sur le site http://support.fortinet.com.

Seuls les administrateurs FortiGate (dont le profil prévoit tous les droits d'accès en lecture et écriture du système) et les utilisateurs admin FortiGate peuvent modifier le logiciel FortiGate.

Après avoir téléchargé une image logicielle FortiGate de Fortinet, les procédures reprises dans cette section vous permettront d'installer l'image logicielle sur votre FortiGate-500x.

Cette section parcourt les sujets suivants:

- Mise à jour logicielle
- Retour à une version logicielle antérieure
- Mise à jour logicielle à partir d'un redémarrage système et par ligne de commande
- Test d'une nouvelle version logicielle avant son installation

Remarque : Si vous avez une version antérieure du logiciel FortiOS, par exemple FortiOS v2.50, procédez à la mise à jour vers FortiOS v2.8MR10 ou v2.8MR11 avant la mise à jour vers FortiOS v3.0.

Mise à jour logicielle

Vous pouvez utiliser, au choix, l'interface d'administration web ou l'interface de ligne de commande pour la mise à jour logicielle FortiOS.

Mise à jour logicielle à partir de l'interface d'administration web

Les procédures suivantes permettent d'installer une nouvelle version logicielle sur le FortiGate.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*.

Remarque : La procédure suivante nécessite que vous vous connectiez à partir du compte administrateur admin ou d'un compte administrateur qui possède tous les droits d'accès en lecture et écriture de la configuration du système.

Mettre le logiciel à jour à partir de l'interface d'administration web

1. Copiez le fichier de l'image logicielle sur votre poste d'administration.
2. Connectez-vous à l'interface d'administration web en tant qu'administrateur admin.
3. Sélectionnez **Système > Statut**.
4. Dans **Statut > Version de code**, sélectionnez Update (Mettre à jour).
5. Tapez le chemin et le nom de fichier de l'image logicielle, ou sélectionnez « Browse » (Parcourir) pour localiser ce fichier.
6. Cliquez sur OK.

   Le FortiGate-500x télécharge le fichier de l'image logicielle, installe la nouvelle version logicielle, redémarre et affiche la page d'ouverture d'une session FortiGate. Cette procédure prend quelques minutes.
7. Connectez-vous à l'interface d'administration web.
8. Sélectionnez **Système > Statut** et vérifiez la version du code pour vous assurer du succès de l'installation de la mise à jour.
9. Mettez les bases de connaissance antivirus et IPS à jour. Pour plus d'informations sur ce sujet, reportez-vous au *Guide d'Administration FortiGate*.

Mise à jour logicielle à partir de l'interface de ligne de commande

La procédure suivante nécessite un serveur TFTP connecté au FortiGate-500x.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Vous pouvez également utiliser la commande CLI `execute update-now` pour mettre à jour ces définitions. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*.

Remarque : La procédure suivante nécessite que vous vous connectiez à partir du compte administrateur admin ou d'un compte administrateur qui possède tous les droits d'accès en lecture et écriture de la configuration du système.

Mettre le logiciel à jour à partir de l'interface de ligne de commande

1. Assurez-vous que le serveur TFTP est opérationnel.
2. Copiez le fichier de la nouvelle image logicielle sur le répertoire racine du serveur TFTP.
3. Connectez-vous en CLI.
4. Veillez à ce que le FortiGate-500x se connecte bien au serveur TFTP.

   Vous pouvez utiliser la commande suivante pour lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :

   ```
   execute ping 192.168.1.168
   ```
5. Entrez la commande suivante pour copier l'image logicielle du serveur TFTP vers le FortiGate-500x :

   ```
   execute restore image <name_str> <tftp_ip4>
   ```

où <name_str> est le nom du fichier de l'image logicielle, et <tftp_ip> est l'adresse IP du serveur TFTP. Par exemple, si le nom du fichier de l'image logicielle est FGT_5001-v30-build200-FORTINET.out et l'adresse IP du serveur TFTP est 192.168.1.168, entrez :

```
execute restore image FGT_5001-v30-build200-FORTINET.out
192.168.1.168
```

Le FortiGate-500x répond par le message suivant:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

A savoir :

```
Cette opération va remplacer la version logicielle actuelle !
Voulez-vous continuer ? (oui/non)
```

6 Tapez y.

Le FortiGate télécharge le fichier de l'image logicielle, met à jour la version logicielle et redémarre. Cette procédure prend quelques minutes.

7 Reconnectez-vous en CLI.

8 Pour vous assurer du succès de l'installation de l'image logicielle, entrez :

```
get system status
```

9 Mettez les bases de connaissance antivirus et IPS à jour. Pour ce faire, entrez :

```
execute update-now
```

Lire également à ce propos le *Guide d'Administration FortiGate*.

Retour à une version logicielle antérieure

Les procédures suivantes permettent d'équiper le FortiGate-500x d'une version antérieure du logiciel.

Vous pouvez utiliser, au choix, l'interface d'administration web ou l'interface de ligne de commande pour retourner à une version précédente du logiciel. Cette procédure restaure la configuration par défaut du FortiGate-500x.

Retour à une version logicielle antérieure à partir de l'interface d'administration web

Les procédures suivantes entraînent la restauration de la configuration par défaut sur le FortiGate-500x et la suppression des signatures personnalisées IPS, de la base de données de filtrage web et antispam et des changements apportés aux messages de remplacement.

Avant de commencer ces procédures, il est recommandé de :

- sauvegarder la configuration du FortiGate-500x
- sauvegarder les signatures personnalisées IPS

- sauvegarder la base de données de filtrage web et antispam

Pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate*.

Si vous retournez à une version antérieure FortiOS (par exemple, passer de FortiOS v3.0 à FortiOS v2.80), la configuration antérieure risque de ne pas pouvoir être restaurée à partir de la sauvegarde du fichier de configuration.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*.

Remarque : La procédure suivante nécessite que vous vous connectiez à partir du compte administrateur admin ou d'un compte administrateur qui possède tous les droits d'accès en lecture et écriture de la configuration du système.

Retourner à une version logicielle antérieure à partir de l'interface d'administration web

1. Copiez le fichier de l'image logicielle sur votre poste d'administration.
2. Connectez-vous à l'interface d'administration web du FortiGate.
3. Sélectionnez **Système > Statut**.
4. Dans **Statut > Version du code**, sélectionnez « Update » (Mettre à jour).
5. Tapez le chemin et le nom du fichier de l'image logicielle, ou sélectionnez « Browse » (Parcourir) pour localiser ce fichier.
6. Cliquez sur OK.

   Le FortiGate-500x télécharge le fichier de l'image logicielle, retourne à la version antérieure du logiciel, redémarre et affiche la page d'ouverture d'une session FortiGate. Cette procédure prend quelques minutes.
7. Connectez-vous à l'interface d'administration web.
8. Sélectionnez **Système > Statut** et vérifiez la version du code pour vous assurer du succès de l'installation du logiciel.
9. Restaurez votre configuration.

   Pour plus d'informations sur la restauration de votre configuration, reportez-vous au *Guide d'Administration FortiGate*.
10. Mettez à jour les bases de connaissance antivirus et IPS.

    Pour plus d'informations sur les définitions des antivirus et attaques, reportez-vous au *Guide d'Administration FortiGate*.

Retour à une version logicielle antérieure à partir de l'interface de ligne de commande

Cette procédure entraîne la restauration de la configuration par défaut sur le FortiGate-500x et la suppression des signatures personnalisées IPS, de la base de données de filtrage web et antispam et des changements apportés aux messages de remplacement.

Avant de commencer cette procédure, il est recommandé de :

- sauvegarder la configuration du système FortiGate-500x en entrant la commande
  `execute backup config`
- sauvegarder les signatures personnalisées IPS en entrant la commande
  `execute backup ipsuserdefsig`
- sauvegarder la base de données de filtrage web et antispam

Pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate*.

Si vous retournez à une version antérieure FortiOS (par exemple, passer de FortiOS v3.0 à FortiOS v2.80), la configuration antérieure risque de ne pas pouvoir être restaurée à partir de la sauvegarde du fichier de configuration.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*. Vous pouvez également entrer la commande `execute update-now` pour mettre les bases de connaissance antivirus et IPS à jour.

Remarque : La procédure suivante nécessite que vous vous connectiez à partir du compte administrateur admin ou d'un compte administrateur qui possède tous les droits d'accès en lecture et écriture de la configuration du système.

La procédure suivante nécessite un serveur TFTP connecté au FortiGate-500x.

Retourner à une version logicielle antérieure à partir de l'interface de ligne de commande

1. Assurez-vous que le serveur TFTP est opérationnel.
2. Copiez le fichier de l'image logicielle sur le répertoire racine du serveur TFTP.
3. Connectez-vous en CLI.
4. Veillez à ce que le FortiGate-500x se connecte bien au serveur TFTP.

   Vous pouvez utiliser la commande suivante pour lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :

   ```
   execute ping 192.168.1.168
   ```
5. Entrez la commande suivante pour copier l'image logicielle du serveur TFTP vers le FortiGate-500x :

   ```
   execute restore image <name_str> <tftp_ipv4>
   ```

   où `<name_str>` est le nom du fichier de l'image logicielle, et `<tftp_ip>` est l'adresse IP du serveur TFTP. Par exemple, si le nom du fichier de l'image logicielle est `FGT_5001-v280-build158-FORTINET.out` et l'adresse IP du serveur TFTP est 192.168.1.168, entrez :

   ```
   execute restore image FGT_5001-v280-build158-FORTINET.out
   192.168.1.168
   ```

Le FortiGate-500x répond par le message suivant:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

A savoir :

```
Cette opération va remplacer la version logicielle actuelle !
Voulez-vous continuer ? (oui/non)
```

6 Tapez y.

Le FortiGate-500x télécharge le fichier de l'image logicielle. Après le téléchargement du fichier un message similaire à celui ci-dessous s'affiche :

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

A savoir:

```
Image bien reçue du serveur tftp.
Contrôle de l'image OK.
Cette opération va rétrograder votre version logicielle
actuelle !
Voulez-vous continuer ? (oui/non)
```

7 Tapez y.

Le FortiGate-500x retourne à l'ancienne version logicielle, restaure la configuration par défaut et redémarre. Cette procédure prend quelques minutes.

8 Reconnectez-vous en CLI.

9 Pour vous assurer du succès du téléchargement de l'image logicielle, entrez :

```
get system status
```

10 Pour restaurer votre configuration précédente, si nécessaire, utilisez la commande :

```
execute restore config <name_str> <tftp_ip4>
```

11 Mettez les bases de connaissance antivirus et IPS à jour à partir de l'interface de ligne de commande, en entrant :

```
execute update-now
```

Egalement, pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate*.

Mise à jour logicielle à partir d'un redémarrage système et par ligne de commande

Cette procédure permet d'installer un logiciel spécifié et de restaurer la configuration par défaut du FortiGate-500x. Vous pouvez utiliser cette procédure pour mettre à jour une version logicielle, retourner vers une version antérieure ou encore réinstaller la version actuelle.

Remarque : Cette procédure diffère en fonction des versions BIOS FortiGate. Ces différences, lorsqu'elles sont d'application, sont précisées dans les étapes concernées de la procédure ci-dessous. La version du BIOS du FortiGate-500x peut être visualisée par une connexion en port console lors du redémarrage du FortiGate.

Cette procédure nécessite :

- Un accès en CLI via une connexion au port de la console FortiGate avec un câble null-modem.
- L'installation d'un serveur TFTP auquel vous pouvez vous connecter à partir de l'interface interne du FortiGate. Ce serveur doit être sur le même sous-réseau que l'interface interne.

Avant de commencer cette procédure, il est recommandé de :

- sauvegarder la configuration du FortiGate-500x
- sauvegarder les signatures personnalisées IPS
- sauvegarder la base de données de filtrage web et antispam

Pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate.*

Si vous retournez à une version antérieure FortiOS (par exemple, passer de FortiOS v3.0 à FortiOS v2.80), la configuration antérieure risque de ne pas pouvoir être restaurée à partir de la sauvegarde du fichier de configuration.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*.

Mettre à jour une version logicielle à partir d'un redémarrage système

1. Connectez-vous en CLI en utilisant les ports du câble null-modem et de la console FortiGate.
2. Assurez-vous que le serveur TFTP est opérationnel.
3. Copiez le fichier de la nouvelle image logicielle sur le répertoire racine du serveur TFTP.
4. Veillez à ce que l'interface interne soit connectée au même réseau que le serveur TFTP.

5 Pour vous assurer de la connexion du FortiGate-500x au serveur TFTP, utilisez la commande suivante pour lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :

```
execute ping 192.168.1.168
```

6 Entrez la commande suivante pour redémarrer le FortiGate-500x.

```
execute reboot
```

Le FortiGate-500x répond par le message suivant:

```
This operation will reboot the system!
Do you want to continue? (y/n)
```

A savoir :

```
Cette opération va réinitialiser le système !
Voulez-vous continuer ? (oui/non)
```

7 Tapez y.

Pendant le démarrage du FortiGate-500x, une série de messages s'affiche sur l'écran.

Appuyez immédiatement sur une touche du clavier pour interrompre le démarrage du système lorsqu'un des messages suivants apparaît :

- Pour un FortiGate-500x muni d'un BIOS v2.x

```
Press Any Key To Download Boot Image ....
..
```

- Pour un FortiGate-500x muni d'un BIOS v3.x

```
Press any key to display configuration menu ..............
......
```

Remarque : Vous n'avez que 3 secondes pour appuyer sur une touche. Si vous n'appuyez pas à temps, le FortiGate-500x se réinitialise et vous devez ré-entrer dans le système et recommencer la commande `execute reboot`.

Si vous avez interrompu avec succès le processus de démarrage, un des messages suivants apparaît :

- Pour un FortiGate-500x muni d'un BIOS v2.x

```
Enter TFTP Server Address [192.168.1.168]:
```

Passez alors au point 9.

- Pour un FortiGate-500x muni d'un BIOS v3.x

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G, F, Q, or H:
```

8 Tapez `G` pour accéder à la nouvelle image logicielle à partir du serveur TFTP.

Le message suivant apparaît :

```
Enter TFTP server address [192.168.1.168]:
```

9 Entrez l'adresse du serveur TFTP et appuyez sur la touche Enter :

Le message suivant apparaît :

```
Enter Local Address [192.168.1.188]:
```

10 Entrez une adresse IP que le FortiGate-500x peut utiliser pour se connecter au serveur TFTP. Il peut s'agir de n'importe quelle adresse IP valide pour le réseau auquel est connectée l'interface. Veillez à ne pas entrer une adresse IP d'un autre équipement de ce réseau.

Le message suivant apparaît :

```
Enter File Name [image.out]:
```

11 Entrez le nom de fichier de l'image logicielle et appuyez sur Enter.

Le serveur TFTP télécharge le fichier sur le FortiGate-500x et un message similaire apparaît :

- Pour un FortiGate-500x muni d'un BIOS v2.x

  ```
  Do You Want To Save The Image ? [Y/n]
  ```

  Tapez `Y`.

- Pour un FortiGate-500x muni d'un BIOS v3.x

  ```
  Save as Default firmware/Run image without saving:[D/R]
  ```

  ou

  ```
  Save as Default firmware/Backup firmware/Run image without
  saving: [D/B/R]
  ```

12 Tapez `D`.

Le FortiGate-500x installe la nouvelle image logicielle et redémarre. L'installation peut prendre plusieurs minutes.

Restauration de la configuration précédente

Si nécessaire, modifiez l'adresse de l'interface interne via la commande CLI suivante :

```
config system interface
     edit internal
        set ip <address_ip4mask>
        set allowaccess {ping https ssh telnet http}
     end
```

Après avoir modifié l'adresse de l'interface, vous pouvez accéder au FortiGate-500x à partir de l'interface graphique et restaurer la configuration :

- Restaurer la configuration du FortiGate-500x
- Restaurer les signatures personnalisées IPS
- Restaurer le filtrage web
- Restaurer la base de données de filtrage antispam
- Mettre à jour les bases de connaissance antivirus et IPS

Pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate*.

Si vous retournez à une version antérieure FortiOS (par exemple, passer de FortiOS v3.0 à FortiOS v2.80), la configuration antérieure risque de ne pas pouvoir être restaurée à partir de la sauvegarde du fichier de configuration.

Test d'une nouvelle version logicielle avant son installation

Vous pouvez tester une nouvelle version logicielle en l'installant en mémoire lors du redémarrage système. Après avoir accompli cette procédure, le FortiGate-500x opère sous la nouvelle version logicielle avec la configuration actuelle. Cette nouvelle version n'est pas installée définitivement. Au prochain démarrage du FortiGate-500x, celui-ci opèrera sous la version logicielle d'origine avec sa configuration actuelle. Si la nouvelle version logicielle fonctionne bien, vous pouvez l'installer définitivement en suivant la procédure « Mise à jour logicielle » à la page 74.

Il est recommandé d'utiliser cette procédure de test avant d'installer une nouvelle version logicielle. Pour appliquer cette procédure, vous avez besoin de vous connecter en CLI via le port de la console FortiGate et le câble null-modem ou câble série RJ-45 <> DB-9 requis par votre modèle FortiGate-500x. Cette procédure installe temporairement une nouvelle version logicielle sous votre configuration actuelle.

Cette procédure nécessite :

- Un accès en CLI en connectant le port de la console FortiGate avec un câble null-modem.
- L'installation d'un serveur TFTP connecté à l'interface interne du FortiGate. Ce serveur doit être sur le même sous-réseau que l'interface interne

Tester une version logicielle

1. Connectez-vous en CLI en utilisant le câble null-modem et le port de la console FortiGate.
2. Assurez-vous que le serveur TFTP est opérationnel.
3. Copiez le fichier de la nouvelle image logicielle sur le répertoire racine du serveur TFTP.
4. Veillez à ce que l'interface interne soit connectée au même réseau que le serveur TFTP.

   Vous pouvez lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :

   ```
   execute ping 192.168.1.168
   ```
5. Entrez la commande suivante pour redémarrer le FortiGate-500x :

   ```
   execute reboot
   ```
6. Pendant la réinitialisation du FortiGate-500x, appuyez sur une touche du clavier pour interrompre le démarrage du système. Alors que le FortiGate-500x démarre, une série de messages s'affiche sur l'écran.

   Lorsqu'un des messages suivants apparaît, appuyez immédiatement sur une touche du clavier pour interrompre le démarrage du système :

- Pour un FortiGate-500x muni d'un BIOS v2.x

  ```
  Press Any Key To Download Boot Image ....

  ......
  ```

- Pour un FortiGate-500x muni d'un BIOS v3.x

  ```
  Press any key to display configuration menu .....
  ......
  ```

Remarque : Vous n'avez que 3 secondes pour appuyer sur une touche. Si vous n'appuyez pas à temps, le FortiGate-500x se réinitialise et vous devez ré-entrer dans le système et recommencer la commande `execute reboot`.

7 Si vous avez interrompu avec succès le processus de démarrage, un des messages suivants apparaît :

- Pour un FortiGate-500x muni d'un BIOS v2.x

  ```
  Enter TFTP Server Address [192.168.1.168]:
  ```

  Passez alors au point 9.

- Pour un FortiGate-500x muni d'un BIOS v3.x

  ```
  [G]: Get firmware image from TFTP server.
  [F]: Format boot device.
  [Q]: Quit menu and continue to boot with default firmware.
  [H]: Display this list of options.

  Enter G, F, Q, ou H:
  ```

8 Tapez `G` pour accéder à la nouvelle image logicielle à partir du serveur TFTP.

Le message suivant apparaît :

```
Enter TFTP server address [192.168.1.168]:
```

9 Entrez l'adresse du serveur TFTP et appuyez sur la touche Enter :

Le message suivant apparaît :

```
Enter Local Address [192.168.1.188]:
```

10 Entrez une adresse IP que le FortiGate-500x peut utiliser pour se connecter au serveur TFTP.

L'adresse IP doit se trouver sur le même réseau que le serveur TFTP. Cependant, veillez à ne pas entrer une adresse IP d'un autre équipement de ce réseau.

Le message suivant apparaît :

```
Enter File Name [image.out]:
```

11 Entrez le nom de fichier de l'image logicielle et appuyez sur la touche Enter.

Le serveur TFTP télécharge le fichier sur le FortiGate-500x et un message similaire apparaît :

- Pour un FortiGate-500x muni d'un BIOS v2.x

  ```
  Do You Want To Save The Image ? [Y/n]
  ```

  Tapez `n`.

- Pour un FortiGate-500x muni d'un BIOS v3.x

  ```
  Save as Default firmware/Run image without saving:[D/R]
  ```

  ou

  ```
  Save as Default firmware/Backup firmware/Run image without
  saving: [D/B/R]
  ```

12 Tapez R.

L’image logicielle est installée en mémoire et le FortiGate-500x fonctionne sous la nouvelle version logicielle, mais avec sa configuration actuelle.

13 Vous pouvez vous connecter en CLI ou à l’interface d’administration web en utilisant n’importe quel compte administrateur.

14 Pour vous assurer du succès du téléchargement de la nouvelle image logicielle, entrez à partir des commandes CLI :

```
get system status
```

Vous pouvez maintenant tester la nouvelle image logicielle.

Index

—A—

ajout d'un serveur override 71–72
ajout d'une route par défaut 60, 62
alimentation du châssis 38–39
avertissements et précautions 16

—C—

carte de commutation FortiGate-5003 27
cavaliers, paramétrage 31
certificat de sécurité 44
circulation de l'air 30
CLI
  connexion 46
configuration
  DHCP 58
  en mode NAT/Route 49
  en mode Transparent 51
  PPPoE 58
configuration par défaut
  des profils de protection 52
  du pare-feu 51
connexion
  à l'interface d'administration web 43
  à partir de l'interface de ligne de commande 46
contrôleur de gestionnaire de châssis 28
  commandes CLI 36
  connexion 35–36

—D—

date et heure
  paramétrage 68
décharges électrostatiques 16
DHCP
  configuration 58
distribution de courant 40–41

—E—

échangeabilité à chaud des modules 46–47
enregistrement du FortiGate 69
environnement, spécifications 35

—F—

FortiGate
  documentation 13
FortiGate série 5000, châssis et modules 17
Fortinet
  Base de Connaissance 13–14
  Service clientèle et support technique 14

Fortinet, gamme de produits
FortiAnalyser ... 8
FortiBridge ... 8
FortiClient ... 7
FortiGuard ... 7
FortiMail ... 7
FortiManager ... 8
FortiReporter ... 8
FortiOS
distribution internationale et américaine ... 6
fuseaux horaires ... 68

—G—

gestionnaire de châssis FortiGate, installation ... 34

—I—

interface d'administration web
connexion ... 43
interface de ligne de commande
connexion ... 46

—L—

logiciel FortiGate
mise à jour ... 73
mise à jour
à partir de l’interface d’administration web ... 73
mise à jour
à partir de l’interface de ligne de commande ... 74
retour à une version antérieure ... 75
retour à une version antérieure
à partir de l’interface d’administration web ... 75
retour à une version antérieure
à partir de l’interface de ligne de commande ... 76
test d'une nouvelle version avant son installation ... 82
logiciel FortiGate, mise à jour ... 73

—M—

mise à jour
des signatures antivirus et IPS ... 69
à partir de l'interface d'administration web ... 69–70
programmation ... 70–71
des signatures IPS
à partir de l'interface de ligne de commande ... 70
mise à jour logicielle ... 73
mise à jour logicielle
à partir de l’interface d’administration web ... 73
mise à jour logicielle
à partir de l’interface de ligne de commande ... 74
mise à jour logicielle
à partir d’un redémarrage système et par ligne de commande ... 78–79
mode NAT/Route ... 54
à partir de l'interface d'administration web ... 59
à partir de l'interface de ligne de commande ... 60–61
paramètres ... 58

mode Transparent 56
à partir de l'interface d'administration web 65
à partir de l'interface de ligne de commande 66
paramètres 65
module de conversion d'alimentation FortiGate-5053 41
montage et installation 30

—N—

NAT/Route, mode 54
NTP, serveur
synchronisation 68

—P—

paramétrage par défaut
restauration 52–53
pare-feu
configuration par défaut 51
PPPoE
configuration 58
précautions et avertissements 16
prise de terre 16
produits de la gamme FortiGate série 5000 17
produits de la gamme Fortinet 7
profils de protection 52

—R—

ram dimm, installation 30
remplacement des modules 46–47
réseau, configuration 54
restauration
du paramétrage par défaut 52–53
restauration de la configuration précédente 81
retour à une version logicielle antérieure 75
à partir de l'interface d'administration web 75
à partir de l'interface de ligne de commande 76

—S—

service clientèle et support technique 14
SFP, transmetteurs 31
synchronisation des date et heure
avec un serveur NTP 68

—T—

tableau de bord 44–45
transmetteurs SFP, installation 31
Transparent, mode 56

—V—

variables d'environnement 35
ventilateur 29–30